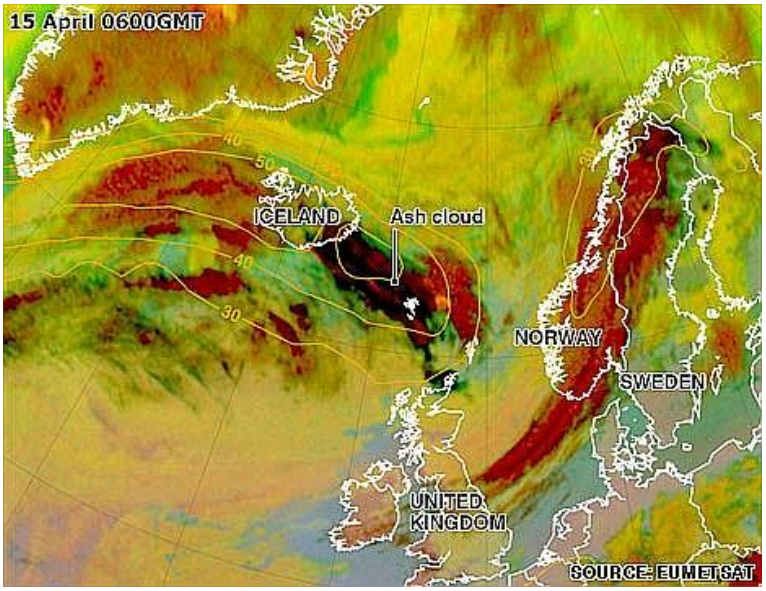
Guideline

CRISIS RESPONSE PLANNING MANUAL (CRPM) - **Part 3** / **Volume 1**

Business Continuity Management - in an Aviation Context

Background / Introductory Information



Volcanic ash cloud plume - Icelandic volcano EYJAFJALLAJOEKULL - 15 Apr 2010 (© EUMET SAT 2010)

The threat to flight operations from the ash cloud referred to above led to the total closure of much of Northern European airspace for almost a week - with combined losses of around $2 billion+ US dollars, due 'business disruption' to affected ***aircraft*** and ***airport*** operators, ***ground handlers***, tour operators / travel & vacation companies etc.

This was the biggest closure of airspace since the end of the Second World War. The associated (knock-on) adverse impacts on flight operations rapidly spread worldwide

A month later a similar ash cloud (from the same volcano) led to a major suspension of flight operations to / from and within parts of Spain and all of the Canary and Madeira islands

EYJAFJALLAJOEKULL volcano April 2010 - © Unknown

© - unknown

To be of any practical use this (two volume) guideline document should be accompanied by an associated and appropriate course of training. To adequately 'train' for what is covered herein, it is envisaged that **AT LEAST *5 full day's training*** is required

For aviation related users / readers - said training **MUST** be delivered by an appropriately competent, experienced person (with regard to Business Continuity and related matters) - who **ALSO** has the appropriate, **AVIATION** related background & experience

Revision Information

This CRPM Part 3 / ***Volume 1*** document comprises 138 pages - all dated 10 March 2020

Revision No	Date	By
* Revision (Original)	30 Jul 2010	A H Williams (author / owner)
** Revision 1	01 Oct 2012	A H Williams
** Revision 2	01 Sep 2014	A H Williams
** Revision 3	01 May 2016	A H Williams
** Revision 4	01 March 2017	A H Williams
** Revision 5	01 March 2018	A H Williams
** Revision 6	01 May 2019	A H Williams
*** Revision 7	10 March 2020	A H Williams

* Based generally on **BS 25999** (ISO 22301 / ISO 22313 formally superseded BS25999 on 01 June 2014)

** Guided ***to a degree*** by **ISOs 22301:2012** & **ISO 22313:2012**

*** Up to early 2020 the contents of this document (CRPM Part 3 / Volume 1) formed part of what was then a ***single*** document of ***300+*** pages - entitled simply ***CRPM Part 3***

With the issue of ISO 22301:2019 and 22313:2020 around late ***2019*** / early ***2020*** respectively - the author owner of the CRPM Part 3 document decided to split the latter into **two**, **separate** volumes. ***Volume 1*** (you are reading it right now) covers general, introductory and background material - whilst ***Volume 2*** (a separate document) provides the associated 'detail'

This document shall be reviewed and revised by its author / owner on an 'as required' basis - being at least 6 monthly. Should a review result in the need for a revision - the latter shall be actioned and the associated controlled document information updated accordingly

Note that each time that a revision is incorporated - the ***entire*** document will be re-issued electronically - with the revision already having been incorporated by the author / owner

The current (latest revision included) version of ***this*** document can always be found at:

https://www.aviationemergencyresponseplan.com/guideline-template/

'CRPM **Part 3** / **Vol 1** - **Intro** to **Aviation Related Business Continuity Planning**'

Any hard copies made of this document should be regarded as uncontrolled - unless the entity / person so doing has taken appropriate action to ensure that the hard copy may be regarded as 'controlled' - within their own sphere of operation - whatever that might be

Control of Documented Information

See (***separate*** document in this series) CRPM Part 3 / Volume ***2*** - pages 58 and 113 - ***before*** starting any tasks / work associated with CRPM Part 3 in general

Acronyms / Abbreviations

BC	Business Continuity
BCPM	BC Programme Management
BCMS	BC Management System
BCP	Business Continuity Plan
BCT	Business Continuity Team
BIA	Business Impact Analysis
BRP	Business Recovery Plan
BRT	Business Recovery Team
CIQ	Customs, Immigration & Quarantine (Port Health) Services (aviation context)
DMC	Disruption Management Centre
DSU	Disruption Support Unit (see also IBU)
ERP	Emergency (Crisis / Incident etc) Response Plan
ERT	Emergency (Crisis / Incident etc) Response Team
GHA	Ground Handling Agent (Airline Representative)
IBU	Individual Business Unit (being part of a larger / parent etc. entity) (see also DSU)
ICAO	International Civil Aviation Organisation (a United Nations entity)
ICT	Information and Communications Technology
IRS	Incident Response Structure
ISO	International Organisation for Standardisation
MAO	Maximum Acceptable Outage (i.e. a period of time) (see also MTPD)
MBCO	Minimum Business Continuity Objective (operationally related level of continuity - as related to provision of product, services etc. - during a disruption type event)
MMS	Modern Management System
MRO	(Aircraft) Maintenance, Repair and Overhaul Organisation
MTDL	Maximum Tolerable Data Loss (relating specifically to data & documentation ***only***)
MTPD	Maximum Tolerable Period of Disruption (re a product, service, activity etc.)
RA	Risk Assessment
RCA	Resources Consolidation Analysis
RM	Risk Management
RPO (CDP)	Recovery Point Objective (**C**ritical **D**ata **P**oint if relating to data/documentation)
RTO	Recovery Time Objective
SMS	Safety Management System
SPOF	Single Point of Failure
TM	Organisation's Top Manager / Top Management Team

This **CRPM Part 3** guideline document (you are reading 'Volume 1' of the latter right now) plus the accompanying / associated (but separate) Volume 2 - describes 'what needs to be accomplished' to successfully introduce a 'fit for purpose' **Business Continuity *Management System*** into an 'organisation'

Where appropriate, said 'organisation' has been put into an ***aviation context*** e.g. as might typically be useful to facilitate business continuity type matters e.g. for ***airlines***, ***airports***, ***ground handling*** operators etc.

This Volume 1 provides general background material only - designed to 'set the scene' for the necessary detail which follows in the ***separate*** Volume 2

See pages 6 to 28 following for a series of images portraying concisely some of the most likely ***threats*** / *hazards* (and thus potential ***risks***) to aviation related organisations - most particularly (for the latter) those concerned in one way or another with aviation related flight operations - typically airlines, airports, ground handling agents etc. Page by page these threats / hazards relate to the general areas of (in no particular order and the list is ***not*** exhaustive):

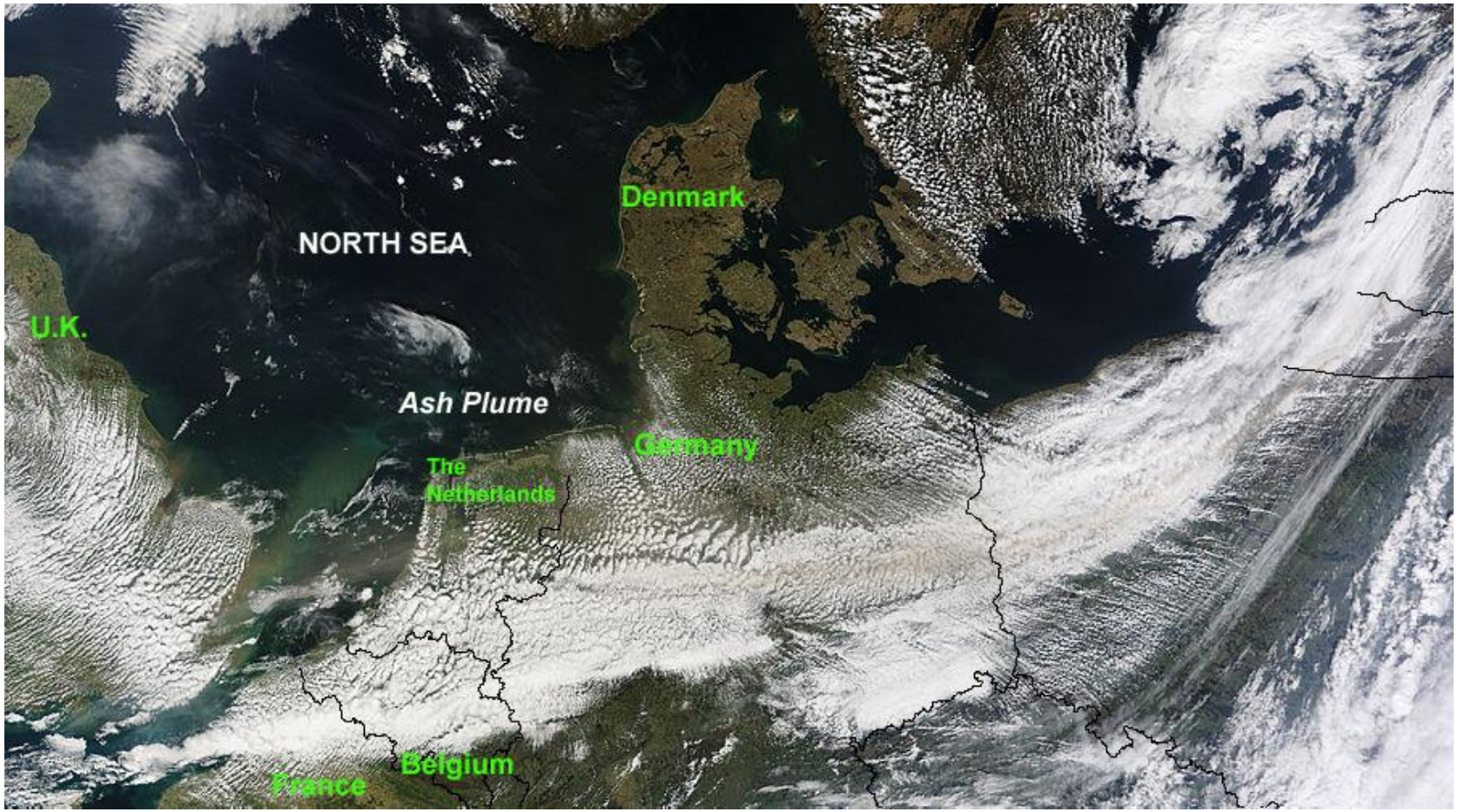
- Page 6 / Fire
- Page 7 / Crime (General)
- Page 8 / Crime (Cyber)
- Page 9 / Public Utilities & Services etc.
- Page 10 / Supply Chain
- Page 11 / Industrial Action and other 'losses of workforce'
- Page 12 / Manmade Disaster (also involving Brand / Image / Reputation issues)
- Pages 13 & 14 / Media (Crisis Communications e.g. 'main' media and social media)
- Page 15 / Financial
- Page 16 / Conflict, War etc.
- Page 17 / Public Health
- Pages 18 to 22 / Natural Disaster; Weather etc.
- Page 23 / Essential Infrastructure; Services; Equipment; Buildings etc.
- Pages 24 & 25 / Safety & Security; Unlawful Interference etc.
- Page 26 / Legal, Statutory, Regulatory etc.
- Page 27 / Customer Service
- Page 28 / Operational Efficiency

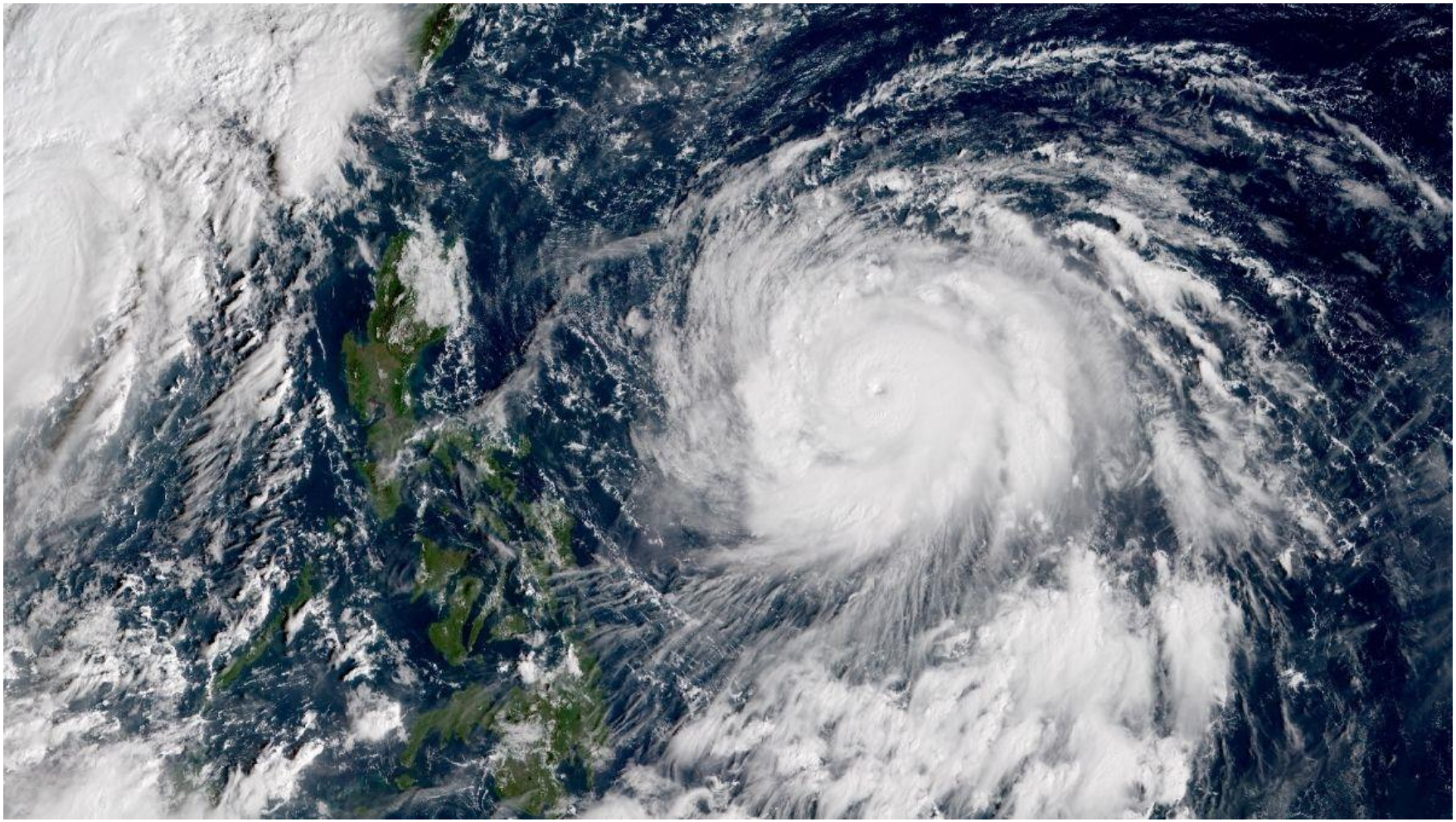
Note: The '**Risk Management**' 'concept of operations' relates to there being several top level (strategic) methods of trying to deal with 'risk'. With one exception they are all ***pro-active*** i.e. attempting to stop / mitigate particular risks from being **realised** (happening) in the first place

The exception relates to mitigating (reducing) the adverse consequences of **realised** risk (i.e. after 'whatever it is' has actually happened) and trying to get things 'back to normal' as quickly as possible. This latter is known as '**Business Continuity**' - and ***is*** the main subject of CRPM Part 3 / Volumes 1 and 2

Deepwater Horizon Oil-spill (Gulf of Mexico) - started 20 April 2010

Man-made disaster + serious brand / image / reputation type issues for BP (British Petroleum)



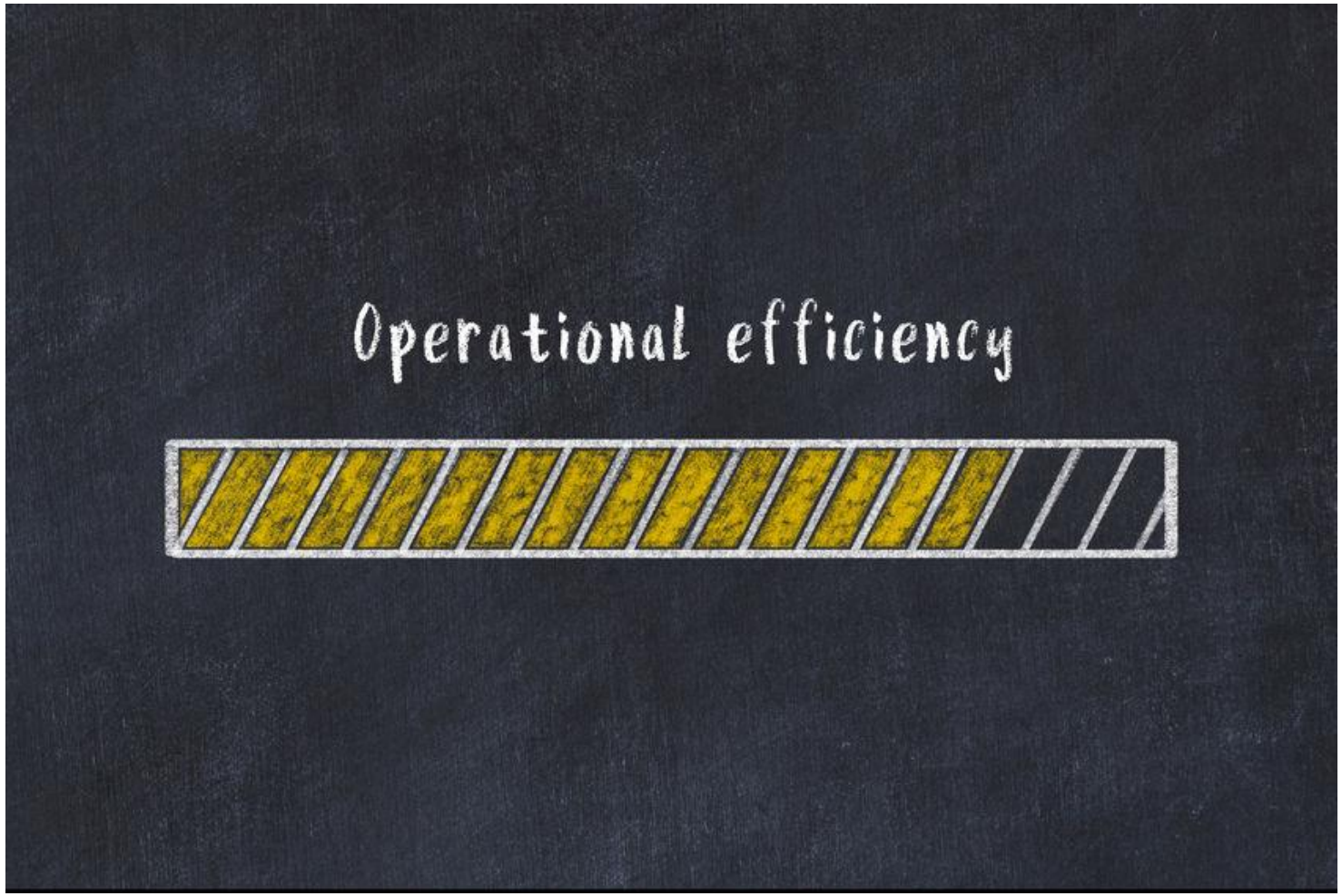


Airport - Automated Baggage Handling System

(1) **Malaysian Airlines Flight MH 370** (disappeared 8 March 2014)

(2) **Malaysian Airlines Flight MH 370** (disappeared 8 March 2014)

- **https://www.youtube.com/watch?v=dJaXb4s3yxc**



Contents

Preamble - please read the following 'orientation' notes (pages 30 - 41) before proceeding further. The notes apply to **CRPM Part 3**, ***Volume 1*** (you are reading the latter right now) **AND** also to ***Volume 2*** (separate document / awaiting issue) - as applicable / appropriate

Note 1 - The user / reader should clearly understand that actually putting the theory contained in this (2 volume) CRPM Part 3 guideline into real (actual) practice, from the 'ground up' (i.e. build, operate and maintain an actual business continuity management system * (***BCMS***) - for a large / complex airline, airport, ground handling operator etc.) is a major undertaking, requiring significant (e.g. up to one year's +) work and the provision of considerable resources

This assumes that just one or two persons (e.g. typically the '***Business Continuity*** [***BC***] ***Manager***' + the alternate / back-up person [or equivalent(s)] - if any) are assigned primary responsibility for the task

* For a ***glossary*** of terms used in this guideline - see page 54. For ***acronyms*** - see page 4

It is possible that smaller / simpler airlines, airports etc. ***might*** be able to complete the task in a commensurately shorter timescale

Of course, it is not just 'work' that is required to successfully establish a BCMS. For example - genuine, adequate, 'evidenced' and on-going commitment and support from top management will be essential - as will financing, procuring and allocating the considerable resources required, together with the achievement of appropriate levels of required 'competence and skills' (training & exercising) by designated persons etc.

When all of the above (and considerably more) is in place, the BCMS will then require ever on-going maintenance, review and evaluation - including 'compliance' (audit) checks - throughout its entire life-cycle

Note 2 - As the CRPM Part 3 guideline is studied, the user / reader will hopefully come to acknowledge (if not already convinced) that business continuity is now a must for most organisations - from the very smallest / simplest / local - to the most complex / largest / international. However, the concept of BC as a practical 'tool' has been around since mankind first evolved - so nothing new here?

Well, there is actually something new i.e. since the industrial revolution and as part of the current 'technological (ICT) revolution', the risk that ***certain*** organisations will cease operations (for anything other than a ***very*** short period of time) - due to disruption of some type, is simply now ***unacceptable*** to society in general e.g.

- Hospitals
- Emergency Services (Police, Fire & Rescue, Ambulance etc.)
- Utilities (water; electricity; gas etc.)
- Information and *Tele*communications Technology (ICT)

- Distribution & Retail (food, fuel etc.)
- Transport Services
- Banking etc.

For similar political, legal, regulatory, commercial, financial, environmental, societal etc. reasons - BC is also now an essential requirement for the majority of 'organisations' in general (whether they realise it or not!)

For example, ***a large and complex commercial organisation*** (e.g. many airlines, airports and ground handlers) needs to keep 'trading / operating' (at least to a ***pre***-defined and agreed level) - despite any significant service / operational disruptions (which could be caused by many different factors [***threats***] e.g. aircraft accident / incident; poor weather; ICT failure / disruption; utilities failure; industrial action by staff; use of facility denial [e.g. due fire, flood etc.]; security related incidents; public health incidents; natural disaster; failure of supply chain; governance [legislation, regulation etc.] type matters; brand / image / reputation issues; criminal action; breakdown of essential equipment / machinery [e.g. particularly 'automated baggage sorting systems'!] - and so on)

The organisation tries to do this (keep trading / operating) in order to avoid ***unacceptable consequences*** to those having an 'appropriate' interest in what the organisation does / produces / delivers etc. i.e. stakeholders / other interested parties of all types, particularly customers / clients , staff and shareholders. One such 'unacceptable' consequence might ultimately mean going out of business / ceasing to trade

Conversely, now take a ***single person trader*** (say an auto / car repair business) - who might consider that BC is not appropriate for him / her. However, what if:

- The business premises are destroyed by fire etc.
- The trader has an accident - keeping him / her off work for a relatively long period
- A critical part of the utilities(e.g. electricity supply) fails for a significant period
- The external 'auto spare / replacement parts' delivery service ceases operation e.g. due bad weather; fuel shortage, sickness, closing down etc.
- The banking used by the business has a major, longer-term ICT failure / problem
- Another auto repair business opens nearby - offering a 'better value (cheaper)' service with no corresponding degradation of quality etc.

Actually, the employment of BC measures (or, more correctly, the very closely related subject of 'risk management measures' [of which BC is one of several [sub] component parts]) ***is*** applicable to all of the above - and more e.g.

- *The premises are destroyed by fire* (Pre-cover and or mitigate this risk using insurance; fire extinguishers; water sprinkler system etc.)

- *The trader has an accident - keeping him / her off work for a relatively long period* (Cover risk using insurance and / or employ pre-identified contract labour for appropriate period)

- *A critical part of the utilities supply fails i.e. electricity* (Maintain a suitable petrol / diesel generator [+ an adequate supply of fuel for same] on-site)
- *The external 'spare / replacement parts' delivery service ceases operation e.g. due bad weather; going out of business etc.* (Maintain a reasonable 'on-premises' stock of the more common spare parts and / or have several different suppliers [not just the one])
- *The bank used by the business has a major ICT failure for a significant period.* (Use at least one other [different company] bank as part of normal business)
- *Another repair business opens nearby - offering 'better value' services* (Build on your reputation and image e.g. using 'quality at a reasonable price' as the main influence for why current / potential customers should continue to use / consider using the business i.e. try to build and retain a loyal client base. Of course, this should be pro-actively initiated ASAP after starting to trade - and not reactively due not taking BC seriously enough until it might possibly be 'too late'!)

Note 3 - If an organisation (especially a 'larger and / or more complex' organisation) wishes to establish a BCMS for itself today, it may need / wish to refer (to a greater or lesser degree) to the * ***guidance*** contained in the International Organisation for Standardisation's (ISO) BC document - known as ISO 22313:2020

* **Comment 1** - do ***not*** confuse use / context of the word '***guidanc***e' as used just above - with the document (known as a '***guideline***') - which you are reading now. ***They are different!***

Comment 2 -the **ISO 22313:2020** ***guidance standard*** is directly linked to its associated (but ***separate***) BC ***requirements standard*** - **ISO 22301**:2019. The former provides ***guidance*** on how the ***requirements*** of the latter might be met

However, ISO 22313 may also be used to guide any organisation to implement a BCMS, ***independent of*** ISO 22301 ***requirements*** - provided that formal certification to the ISO 22301 standard is ***not*** required

Comment 3 - a whole BC 'vocabulary / terminology' has grown up around ISOs 22313 and 22301 (and their preceding 'national and industry' standards [now largely superseded] - upon which they have largely been based e.g. BS 25999). Accordingly, a significant portion of this vocabulary has been used in this guideline - and the user / reader should become familiar with same if the intention is to set up a BCMS. See Glossary starting on page 54

Comment 4 - a brief overview of the ISO 22313 and ISO 22301 ***standards*** can be found starting page 45

Note 4 - The amount and variety of information contained in this two 'volume' CRPM Part 3 guideline might appear daunting. Indeed, there is a lot to take in. However, keep in mind that:

a. The information provided should be sufficient for larger and / or more complex organisations to obtain & understand ***all*** of the ***working basics*** of what is required in order to prepare, implement, maintain etc. a fit for purpose BCMS i.e. they will typically require 100% *(and more - see note 4c below)* of what is included herein

b. Some medium and most smaller and / or less complex organisations should be able to adapt / cut-down to a significant degree what has been referred to in 4a above, commensurate with their own requirements - and provided that the BCMS essentials are covered (again, we are just referring here to the ***working basics***)

c. Any organisation will need **ALL** of the information contained herein (and more) if it is intended to meet (be ***certificated*** to) the ***requirements*** of BC Standard ISO 22301. The same applies (albeit to a lesser degree) if an organisation intends ***instead*** to make a ***self-determination / self-declaration*** of ***alignment*** with ISO 22313

IMPORTANT: An organisation can plan / implement etc. a BCMS - ***without*** needing ISO 22301 ***certification*** or a ***self-determination*** / ***declaration of alignment*** with ISO 22313. However, such organisation will still generally require some form of guidance in the task - which is where ISO 22313 might be able to help - ***at least to a very limited degree***

When ISO 22301 and ISO 22313 first 'came into being' in 2012 - that was it i.e. there was nothing else (except for the associated glossary contained in a separate ISO publication known then [and now] as ISO 23000). All needed to be purchased (at very expensive prices commensurate to what one was getting in return) from ISO itself or an ISO accredited 'agency' e.g. BSI (British Standards Institute)

The purpose of ISO 22313 is to provide ***guidance*** on how to comply with the ***requirements*** of its associated ISO 22301 standard. ISO 22313:2012 was * significantly ***deficient*** in this matter

In the intervening years up to 2020, ISO had accordingly introduced a series of ***additional***, related guidance documents (again, all requiring additional purchase) - presumably to make up for ISO 22313's shortfall

These 'extra' documents are listed - starting top of next page

* However, do note the following quote from **ISO 22313:2012** ……*"It is not the intention of this International (guidance) Standard to provide general guidance on **all** aspects of business continuity". **In reality, it gave very little guidance at all - and what it did give was far from adequate***

Re the last para above, this situation had ***not*** changed significantly for the better in the ISO 22313:2020 version - (issued Feb 2020)

Note: All comment herein re the efficacy of identified ISO documents is based on the personal (but informed) opinion of the author / owner of the guideline document being read right now

- ISO/TS 22317:2015 - Societal Security ($**138** USD / **27** pages) - *Business continuity management systems - Guidelines for (preparing and conducting) **'business impact analysis'** (BIA)*. Note: TS 22317 relates to ISOs 22301 & 22313

- ISO/TS 22330:2018 - Security and Resilience ($**158** USD / **38** pages) - *Business continuity management systems - Guidelines for **people aspects on business continuity***

- ISO/TS 22331:2018 - Security and Resilience ($**118** USD / **25** pages) - *Business continuity management systems - Guidelines for (preparing and introducing) **business continuity strategy and solutions***. Note: TS 22331 relates to ISOs 22301 & 22313

- If 'supply chain' operations / matters etc. are pertinent - ISO/TS 22318:2015 - Societal Security ($**118** USD / **22** pages) - *Business continuity management systems - Guidelines for **supply chain continuity***. Note: TS 22318 relates to ISOs 22301 & 22313

The above gives a total price of USD $532 (ISO prices as at March 2020) for a total of 112 pages i.e. ***about $5 USD per useful page** [and $10 per useful sheet]*)

An additional document (see below [requires purchase]) is due for issue sometime in 2020:

- ISO/TS 22332:2020 - Security and Resilience ($ TBA USD / TBA pages) - *Business continuity management systems - Guidelines for developing **business continuity plans and procedures** (**expected issue date sometime in 2020**)*. Note: TS 22332 relates to ISOs 22301 & 22313

Oh - and let's not forget the need to also purchase the three BC ***foundation*** documents:

- ISO 22300:2018 - Security and Resilience ($**38** USD / **35** pages) - ***Vocabulary***

- ISO 22301:2019 - Security and Resilience ($**118** USD / **21** pages) - ***the BCMS Standard***

- ISO 22313:2020 Security & Resilience ($**176** USD / **55** pages) - *Business continuity management systems - **Guidance** on / about implementing its related 'requirements' standard (i.e. ISO 22301)*

.....and the ISO 'rip-off' continues as, if one was really serious about doing a 'proper job' of introducing a BCMS into an organisation (according to ISO), one must also get his / her head around certain aspects of '***risk management***'. ISO can help you with this by also selling:

- ISO 31000:2018 - *Risk Management **Guidelines*** ($**88** USD / **16** pages)

- ISO 31010:2019 - *Risk **Assessment Techniques*** ($**198** USD / **264** pages) [the previous {2009} version cost $320 USD for 176 pages - so the 2019 version is a ***relative*** bargain!]

- ISO Guide 73:2009 - *Risk Management **Vocabulary*** ($**88** USD / **15** pages)

- ISO 31073: due to be issued mid to late 2020? (Risk Management Vocabulary) ($TBA / TBA) - *Under development as at early 2020 (should replace ISO Guide 73:2009???)*

Appropriate further expansion / amplification of all of the above (typically contained in independent, ***commercial*** publications - requiring additional purchase) might also be necessary

This latter was originally an essential requirement when ISOs 22301 /22313 were first published in 2012 - as ISO 22313 did ***not*** effectively meet up to its title of being a 'guideline'. However, with the advent of all of the other ISO documents in the BC series being published in the intervening years (see previous page) this is not so necessary today - but is nonetheless still a consideration

Of course, there ***is*** also an absolutely 100% **FREE** resource available which provides what is needed

You are reading (Volume 1 of) **it right now**! It (CRPM Part 3 [2 Volumes] - Business Continuity Operations in an Aviation Context) is about 80% generic and 20% aviation related - so **should still be very useful to most organisations** - even if not aviation related)

See also Appendix E (page 132) to this document

d. Further to note 4c further above, the reader / user might find it useful to be absolutely clear of the relationship between ISO 22301 and ISO 22313

- ***ISO 22301*** is the BCMS standard itself. As such it specifies ***requirements*** that an organisation ***must fully meet*** in order to successfully achieve associated and ***formal*** 'certification' to that standard. Such certification is awarded by a 'certification body' (Note that ISO is ***NOT*** a certification body)

  Certification can add 'credibility' to an organisation e.g. by demonstrating that its product(s), service(s) etc. consistently meets the expectations of associated customers etc. Such credibility can (and often does) mean more customers / business / profits / success etc. - so ***might*** be worth achieving. (**BUT** see also appendix E, Part 2 - starts page 135 - for the 'counter argument / viewpoint')

  Note that almost 24, 000 ISO Standards existed as at early 2020)

  External (to ISO) 'certification bodies' (located worldwide) are responsible for the actual awarding of certification. As with everything else in life, certification bodies can be good, bad or anywhere in between. Consequently it is always advisable to use an '***accredited***' certification body. For more information on the latter contact the national accreditation body in your own country or visit (internet search) the 'International Accreditation Forum'

- ***ISO 22313*** is a ***supporting*** ISO standard which helps (provides ***guidance*** for) organisations undertaking ISO 22301 implementation and (as required) certification. Consequently, an organisation can be certified only against ISO 22301 and ***NOT*** against ISO 22313

Note 5 - To avoid confusion / for the sake of clarity - it must be clearly understood that this 2 volume CRPM Part 3 guideline document (reminder: you are reading 'volume 1' right now) is ***not*** about simply putting together (producing) '***just a business continuity plan***'. Rather, it is meant to give the user / reader a good working knowledge (understanding) of the ***ENTIRE***, overarching process as to how a BCMS might relate to any organisation and, where so desired, then ***used further*** to ***assist*** in guiding the introduction of a BCMS into such organisation

As per above, one (BUT only one of many) BCMS implementation tasks requires the production of an associated **BUSINESS CONTINUITY PLAN** (BCP) i.e. (and to re-iterate) the latter is ***just one*** of the many building blocks (another being e.g. 'personnel competency and experience' - achieved by training and exercising) required to establish a full, successful BCMS. Each and every such building block needs to be addressed ***separately*** i.e. ***in its own right***

Note 6 - Prior to the 2012 introduction of ISOs 22301 & 22313, there were a number of differing and unresolved viewpoints on the subject of 'business continuity' and its '*relationship*' with the separate but closely related subject of 'risk management'

Some of these viewpoints were undoubtedly driven by partisan / vested interests related to one or other of these subjects and the persons practising and / or gaining profit from them!

The relationship is actually quite clear - i.e. business continuity is simply a ***subordinate***, ***component*** (known variously as a 'risk control / treatment / solution') of ***risk management*** i.e.

- ***Threats*** to an organisation are identified, analysed & assessed / evaluated - the evaluated results being expressed in terms / units of level of '***risk***' to the organisation

Note: Above is believed to relate to the year 2018

- An 'informed' decision is then made on what to do with (how to '**control**', '**treat**', '**solve**' etc.) such evaluated ***risk*** - the more obvious options being ignore; avoid; transfer; accept; exploit; ***manage*** / ***mitigate*** / ***reduce*** etc.

- One (but ***only one*** of several - see diagram above) method of managing / mitigating / reducing ***risk*** is to use appropriate ***business continuity*** measures. (A more exacting term [used frequently herein {in this CRPM Part 3}] for 'business continuity measures' is 'business continuity ***tactical*** solutions / treatments / controls'

  The word '***tactical***' was chosen to differentiate this particular activity from something known as * 'business continuity ***strategy***'. More on this when you get about half-way through [*separate* document] CRPM Part 3 / ***Volume 2***)

  Note: The term '***exploit***' (see diagram above) is related to a concept / activity known as '***risk appetite***' (see definitions). Whilst the latter was deemed to have some degree of importance in the 2012 versions of ISOs 22301 and 22313 - the 2019 / 20 versions respectively had (wrongly???) reversed this outlook somewhat with regards to the ***BC viewpoint***

  * "Business Continuity Strategy" was the original term used in the 2012 versions of ISOs 22301 / 22313. In the 2019 / 20 versions respectively it was retitled to "Business Continuity Strategy ***and Solutions***"

The user / reader might ask '*why is this relationship* (between business continuity and risk management) *important?*'

.....and the answer is that business continuity (BC) & risk management (RM) are so interdependently linked that neither can be ignored in their practical application. This is particularly so for BC and its (still historically unacknowledged by some) ***subordination*** to the parent / overarching RM processes

This relationship has always been evident within 'modern' BC - e.g. there is no point in completing a ***Business Impact Analysis*** (an essential BCMS 'building block) unless an associated ***Risk Assessment*** is also undertaken & the results merged and then jointly evaluated and subsequently managed

BUT - the BC 'experts' (originally ISO's Technical Committee [TC] 223 [Societal Security] in 2012 - but [since 2015] undertaken by TC 292 [Security & Resilience]) who put together ISO 22301:20***12*** & ISO 22313:20***12*** unfortunately went beyond ***simple*** risk assessment (which is ***relatively*** easy to understand and implement) and ***significantly complicated matters*** by additionally including the need for: ..... *(Quoting from **ISO 22313:2012 at the time**)*

- Accountabilities and actions relating to 'risk strategy' and 'risk appetite'
- The need to establish a ***formal*** 'risk assessment' process
- The 'strongly implied' need to obtain (buy), refer to (and understand):
    - Risk Management standard 'ISO 31000' (*Risk **Management** - Principles & Guidelines - [2018 version = 16 pages / approximate price USD $88])*
    - 'ISO 31010' (*Guidance on Selection & Application of Risk **Assessment** Techniques - [2019 version = 264 pages / approximate price $198])*
    - ISO Guide 73:2009 *(Risk Management Vocabulary - [16 pages / approximate price USD $88] - [replaced in 2020 by ISO **31073** - price TBA])*

Accordingly, the introduction of ISOs 22301 & 22313 in 2012 effectively placed an additional burden on those persons assigned BC ***responsibilities & accountabilities*** within an organisation - in that such persons might have subsequently been required to achieve a certain degree of RM competence (knowledge & proficiency) and / or access to such competence from an appropriate external source - depending on the organisation's circumstances and resources

For example, where an organisation ***already had*** an effective & efficient RM Department / Business Unit - much if not all of the RM aspects of BC could have been assigned / delegated to that department / business unit. Indeed, many organisations combine the RM & BC functions (or, more realistically, BC is simply seen as a sub-component part of an organisation's overarching RM roles & responsibilities)

However, the major problem concerned organisations wishing to establish / update a BCMS - where no RM expertise was internally available (i.e. beyond the ability to understand & apply ***simple*** risk assessment implementation techniques) - and where lack of appropriate financial resources did not permit engagement of external RM expertise (typically an RM consultant)

Should such organisations desired to have been certificated to ISO 22301 / or guided by ISO 22313 at that time - the job would have been difficult enough if these 'new' BC requirements related to RM had not been there. But they were ..... and in their form (at that time) could be seen to have needlessly over-complicated an already (relatively) complicated process - whilst significantly increasing the already onerous awareness, competence and implementation burdens on those primarily involved

The above situation had not changed significantly with the introduction of ISOs 22301:2019 and 22313:2020 - excepting that the concept of 'risk appetite' had been dropped / ignored

(Note this latter move was a mistake [in the opinion {subjectivity acknowledged} of the author / owner of this CRPM Part 3 / Vol 2 guideline document i.e. the one you are reading now!])

Note 7 - Cross-referencing to ISO 22313 has been used (where thought useful) in CRPM Part 3 - more particularly in Volume 2

It is, therefore, desirable that ready access to at least ISO 22313 (latest [i.e. 2020] version) is available to the 'interested' user / reader (by whatever means are easiest / cheapest / legal etc. [see also the appropriate / associated information found on page 136]) - and that it is then referred to (via the cross references mentioned above) in order to reinforce and supplement (& possibly present slightly differing viewpoints in areas) what has been written herein

As to most of the other ISO documents listed under Note 4 further above (starts page 33) - it is suggested that the information provided in ***this*** CRPM Part 3 / Volume 1 **+** (together with) its corresponding Volume 2 - ***might be considered to be an adequate*** *(and FREE)* ***substitute***

Note 8A

- This original document (the '**work**') contains material protected under International and / or Federal and / or National Copyright Laws & Treaties. Any ***unauthorised*** use of this material is prohibited
- However, all & any entities & persons are licensed / authorised (by the copyright owner / original author of the work) to use the work under the terms of a 'creative commons licence'. (Follow the link below to see the basic terms of this licence in plain language (from there you can then also link to the 'legal' language version)):

  Attribution - Non-Commercial (3.0) Unported Licence - (CC BY-NC 3.0)

  Note - 'attribution' means placing the following (below) text in the header (or some other ***prominent*** position e.g. the page after the title page / front cover) of all and any derivative document(s) (known as 'adaptations') - which you make at any time - as based on this work:

  '© AERPS / MASTERAVCON (A H Williams) - some rights reserved'

- For any *other* use of the work (e.g. use 'for commercial' / 'for profit or reward' purposes) - **written permission is required**. Such permission can be requested from:

  info@aviation-erp.com

- The copyright owner / original author agrees that the term 'commercial' (as used above) can be fairly interpreted as **not** applying to any use of this work as a template / guideline, where such use is made solely (only) for producing an emergency response plan or similar document (including a Business Continuity Plan and similar) - and where such use is solely (only) made by an entity (e.g. an airline, an airport) or a person(s) in the employ of such entity - ***for internal use by such entity alone***

- If derived / adapted / changed versions (*adaptations*) of this work are made, then a statement to this effect must be placed in some appropriate, prominent position (e.g. the page after the title page / front cover) of all and any such derived / adapted / changed versions e.g.

  '.....This is an adaptation of [insert title / name of the work] by [AERPS / MASTERAVCON / A WILLIAMS (copyright owner and author)] .....'

- If ***adaptations*** of this work are made, it is recommended that all images in the original are replaced and / or omitted in the adaptation. This is in order to avoid any potential infringement of image copyright, which the original work copyright owner / author might reasonably be unaware of

- Entities and persons intending to distribute this ***work*** and / or its ***adaptations*** to other entities and persons, shall be responsible for ensuring that the terms, conditions etc. of this 'Note 8A' and the associated 'creative commons licence' referred to above, are passed on in turn. All entities and persons receiving such distributed versions shall then be bound by / subject to these same terms and conditions

Note 8B - Any person / entity having reasonable cause to believe that his / her / its copyright has been infringed in this document (work) - should please contact (email) the author soonest, in order that the issue can be mutually and satisfactorily resolved, without undue delay:

info@aviation-erp.com

Note 9 - An airline requires a suitably effective & efficient method of managing its emergency / crisis / incident / contingency response plans (including its Business Continuity Plan)

A diagrammatic account of the method used in ***this*** series of guideline and guideline / template documents (you are reading one right now) will be found on page 49

The latter is a well tried and proven method and it is recommended that airlines consider adopting same. If done, this will further strengthen the standardisation aspects of emergency /crisis / incident / contingency response plans amongst airlines and between airlines, airports and ground handlers

The above method can similarly be adopted and adapted for ***Ground Handling Operator*** use

However, note that it is **NOT** suitable for ***airport*** business continuity plans - which should be included (instead) as a component (sub) part of the parent '**Airport Emergency Plan - AEP**'

Note 10 - Despite reasonable care being taken in the preparation of this series of guideline and guideline / template documents, they will inevitably contain errors, omissions & oversights, incorrect assumptions, links no longer valid / working etc.

Readers / users identifying same and similar in this particular document (the one you are reading now) are requested to please notify (via email) the author / owner accordingly at - info@aviation-erp.com. Suggestions for improvement will also be gratefully received

Whilst ISO 22313:2020 can be purchased, a thorough internet search (using appropriate keywords and 'know how') ***might*** **come up with what is required at no cost** (such search is likely to become more successful commensurate with the time period passed since the document was first published in February 2020). **However, do keep in mind that all ISO documents etc. are copyright protected, so caution in such matter is advised**

To save a lot of 'hassle' it might be advisable to just purchase ISO 22313 (at time of writing current version was the one published in February 2020) anyway. The 'ISO Store' is one of the easiest ways of doing this and can be cheaper than other 'official sources (e.g. BSI in the UK)

A cheaper alternative might be the Estonian produced version. You can buy it here

https://www.evs.ee/en/iso-22313-2020

Unless intending to certify your BCMS to ISO 22301 ***requirements*** there is little (if any) need to purchase it

See again 'Preamble' Note 4 (starts page 33) and Appendix E (starts page 132) for further guidance on the general subject of whether to purchase (or not) ISO documents regarding BCMS; Risk Management etc.

End of Preamble Section

Deliberately Blank

Concurrent BCP Ops + ERP Ops + Normal Business Ops

(ERP = Emergency Response Plan)

The above subject is outside the scope of ***this*** CRPM Part 3 guideline (latter being the document which you are reading right now)

However, it is important that airlines, airports, GHAs etc. clearly understand the limitations (particularly in terms of lack of competent manpower resources) which will almost certainly be placed upon them when conducting (trying to conduct) such ***concurrent*** ops (as applicable)

Consequently, the author of this guideline has produced a ***separate*** information article designed to assist in 'what might be required' in order to (try to) adequately manage such ***concurrent*** requirements, if / when so needed

Please see (activate the following link):

https://aviationemergencyresponseplan.com/information/

When the associated webpage opens, scroll down until you find the info article entitled:

* Information Article - A proposed method of managing **Concurrent ERP + BCP + Normal Business Ops**

Click on the article to open and read

Deliberately Blank

ISO International Standards for Business Continuity

ISO (Background Information)

ISO (International Organisation for Standardisation) is the world's largest developer of voluntary 'International Standards'. It was founded in 1947, and has subsequently published more than 24,000 International Standards (and growing) covering almost all aspects of technology and business. Around 165 countries are members of ISO

A '**standard**' is a document which provides ***requirements***, ***specifications***, ***guidelines*** *or* ***characteristics*** - and which can be used consistently to ensure that ***materials***, ***products***, ***processes*** *and* ***services*** are fit for their intended purpose

ISO's International Standards require purchase

Some of the first ISO standards issued were in the ISO 9000 (Quality Management) range - with perhaps the best known being 'ISO 9001 - Quality Management System Requirements'

International Standards aim at ensuring that products and services are safe, reliable and of good quality. For business use, they are strategic tools which can reduce costs by minimising waste and errors - and increasing productivity. They can also help organisations to access new markets, level the playing field for developing countries and facilitate free and fair global trade

Note - many countries produce their own ***national*** standards (similar in concept to ISO standards) on a vast range of subjects. Some take guidance from / are similar to ISO standards and some do / are not

In some subject matter areas the best of national standards have been combined to create an equivalent ISO 'international' standard. An excellent example of this relates to ***business continuity planning and operations*** - see below

ISO - ***Business Continuity*** Standards - 2012

Up to 2012 a significant number of countries produced their own national standards relating to the subject of 'business continuity'. In that year most (but not all e.g. the USA) of these national standards were superseded by two new international (ISO) standards:

- **ISO 22301:2012** - 'Security & Resilience' - **B**usiness **C**ontinuity **M**anagement **S**ystems (BCMS) - ***Requirements***

  This standard specified the ***requirements*** for planning, establishing, implementing, operating, monitoring, reviewing, maintaining & continually improving a *documented management system* to better protect against / reduce the likelihood of occurrence / prepare for / respond to and recover from disruptive incidents i.e. a BCMS

How these requirements were to be applied typically depended on the various aspects of a participating organisation's operating environment, the complexity of that organisation - and 'how far it wished to go' along the Business Continuity 'road'

Organisations are re able to apply for certification / accredited certification against this standard and thus demonstrate to legislators, regulators, customers, ***prospective*** customers and other interested parties that they (organisations) are adhering to good Business Continuity Management (BCM) practice

Compliance or alignment with ISO 22301 also enabled the 'business continuity manager / equivalent person' to demonstrate to 'top management' that a recognized BCM level of operation had been achieved within the organisation

ISO 22301 was necessarily formal in style (comprises short, concise ***requirements***) in order to facilitate ***compliance auditing*** and ***formal certification***

However, a more extensive (separate but supporting) guidance standard (ISO 22313:2012 - see next ***main*** bullet point further below) had also been developed in order to provide greater detail (***guidance***) on each ISO 22301 ***requirement***

Potential benefits of adopting the ISO 22301:2012 standard included:

- Identification and management of current and future threats
- Taking a proactive approach to minimizing the impact of incidents on business
- Keeping critical functions up and running during times of crisis
- Minimising downtime during incidents and improving recovery time
- Demonstrating resilience to customers, potential customers, suppliers etc.

- **ISO 22313:2012** - 'Security & Resilience' - Business Continuity Management Systems (BCMS) - ***Guidance***

This standard provided ***guidance*** for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving an associated, documented management system (in this case *ISO 22301*) - thus enabling organisations to better prepare for, respond to and recover from disruptive incidents

It was not the intent of ISO 22313 to imply uniformity in the structure of a BCMS - but rather for an organisation to design a BCMS which was appropriate to its own needs and which met the requirements of associated interested parties / stakeholders - including customers. Such needs being typically shaped by:

- Legal, regulatory, organisational and industry requirements
- The nature of an organisation's product(s) and / or service(s) etc.
- The processes associated with providing the product(s) and / or services etc.
- The organisation's operating environment

- The size, structure and complexity of the organisation
- The organisation's level of 'risk appetite'

ISO 22313 was generic i.e. applicable to all sizes and types of organisation, including large, medium and small entities operating in industrial, commercial, public and not-for-profit etc. sectors - that wished to:

- Establish, implement, maintain and continually improve a BCMS
- Ensure conformance with the organisation's business continuity policy
- * Make a self-determination / self-declaration of compliance or alignment with ISO 22313 - or
- Use the guidance to achieve ISO 22301 certification / accredited certification

* Where so desired, an alternative to *ISO 22301 certification / accredited certification* (the latter typically being a significant [work intensive / time consuming / resource related {including money / finance} etc.] undertaking for many organisations - especially those which are large and / or complex etc.) was for an organisation to formally (or even informally) ***align*** its BCMS with *ISO 22313 guidance* instead. If pursued, the work and other requirements etc. were still considerable, but the associated pressures related to 'certification' no longer applied

ISO - ***Business Continuity*** Standards - **2019** / **20**

There were no hugely significant changes in the October 2019 version of ISO 22301 & the February 2020 version of ISO 22313 - compared with their equivalents published in 2012 or thereabouts

For outline details of what ***did*** change, see again 'Note 4' starting on page 33 - together with the contents of Appendix D (for ISO 22301:2019 only) - starts page 125

Deliberately Blank

ABCX Airways (Preamble 'Note 9' on page 40 refers)

Crisis Response Planning Manual (CRPM)

The CRPM is the 'master' document which regulates and guides **all** forms of crisis / emergency / incident (contingency) response within 'ABCX Airways'

The CRPM is made up of 6 *separate* **Parts** - each part dealing with a specific type / aspect of an emergency / crisis / incident / contingency response - and containing associated accountabilities, procedures, checklists, information, explanations etc. The six 'Parts' of the CRPM are:

CRPM PART 1 - Catastrophic **Aircraft Accident**

CRPM PART 2 - **Aircraft Incidents**

CRPM PART 3 - **Aviation Business Continuity Plan**

CRPM PART 4 - **Public Health** Incident

CRPM PART 5 - **Natural Disaster**

CRPM PART 6 - **Training** Manual

C R P M

Purpose & Scope

The ***purpose*** of the (combined 2 volumes) of CRPM Part 3 is to:

- Provide a suitable reference source related to facilitating the acquisition of a ***reasonable*** level of ***theoretical*** knowledge - re the subject of business continuity in general - and **aviation** related business continuity in particular

The associated ***scope***:

- Provides an appropriate depth and range of material, sufficient to permit a ***foundation*** *(reasonable)* level of potential understanding to be acquired - relating to the concept and general (but not specific) practice of a ***'generic'*** Business Continuity Management System (BCMS) within a generic organisation ..... **AND**
- Relates / translates (where appropriate) this generic BCMS to / into an aviation context
- Does ***NOT*** relate to the ***specific task*** (i.e. the ***actual WORK*** involved) of introducing a BCMS into an organisation (especially where this might be undertaken in conformance with a business continuity standard - e.g. **ISO 22301**) - **BUT** will nevertheless be found to be an extremely useful aid in such task *(see 'Objectives' - next page)*
- Generally excludes (for the sake of clarity, brevity and simplicity) ***business continuity requirements and activities relating to 'data'*** - whether in soft and / or hard copy formats. In reality, however, this latter element of business continuity planning **MUST** be covered of course. The associated concepts / practices are relatively simple to understand and implement e.g.
    - Regular backups made of electronic data
    - Electronic data backups to have an additional (adequate, secure & easily / rapidly accessible) 'off-site' storage capability
    - Hard copy documents to be stored in fire-proof repositories
    - Hard copy documentation of high importance to be copied and additionally stored in an adequate, secure & easily / rapidly accessible 'off-site' facility etc.
- Does ***NOT*** include the 'risk' (and thus [by implication] 'business continuity') aspects of ***aviation*** which relate to ***safety*** (flight safety / safety management) etc. This is because:
    - ICAO Annex 19 (Safety Management) and its related documents (particularly ICAO Doc 9859 - 'Safety Management Manual') are the specialist sources / providers, references etc. of / for information, requirements, processes and procedures etc. in the 'bespoke' area of ***aviation safety related*** '***risk management***' and its derivatives (they cover lots of other thing too, of course)

- Individual UN countries (i.e. at country / state [i.e. government] level) ***must*** comply with appropriate elements (of ICAO Annex 19, Doc 9859 etc.)

  They, in turn, ***must*** provide (within their own jurisdictions) oversight of similar responsibilities for appropriate 'operational type' ***aviation related service providers*** (e.g. involving most Airlines, Airports, GHAs, Maintenance & Repair Organisations, Flight Training Providers etc.) regarding safety management

- Does ***NOT*** include the ***risk*** (and thus [by implication] business continuity) aspects of ***aviation security*** *(AVSEC)*

  AVSEC might be described as ..... 'A combination of human and material resources necessary to safeguard civil aviation against unlawful interference' (e.g. bomb threat, hijack, sabotage, other threats to life / property, communication of a false threat etc.)

Objectives

* ***On successful completion of an appropriate course of training*** (e.g. as associated with the subject matter included in ***this*** complete [2 volume] guideline [CRPM Part 3] document) the typical user should be in a position to progress to the ** 'next phase'

The latter (*next phase*) involves acquisition of the Business Continuity (BC) related ***'on-the job practical experience*** (and / or equivalent)' necessary to eventually conduct effective and efficient **ACTUAL** *(real /practical)* BC activities, particularly with reference to aircraft, airport & other (relevant) aviation related ops

* This guideline can be used as the foundation material for the associated training course

** The 'next phase' (as mentioned in the para above) is ***outside*** the scope of ***this*** CRPM Part 3 Guideline

Context

The majority of CRPM Part 3 has been written in the context of BC activities related to 'generic' organisations. This was deemed necessary in order for the user / reader to build up a solid BC foundation, with the aim of using it to progress (if and as required) to the application of BC in any practical context - ***provided that suitable*** **further** ***training and / or hands-on experience and / or qualification requirements are met***

Selected elements of CRPM Part 3 provide an introduction to BC as it relates specifically to **aviation related** operations. A medium to large sized operator / organisation (airline, airport, GHA etc.) has been assumed for this purpose, unless stated otherwise. However, do note that the business continuity concept can be applied to just about any aviation entity, regardless of what the entity does - and of its complexity and / or size

Vocabulary (Glossary)

The vast majority of information provided in this CRPM Part 3 in general (and Volume 2 in particular) ***relates loosely*** to the current versions (see next paragraph) of (separate [but related to each other] documents) *ISO 22301* and *ISO 22313*

Separate document '***ISO 22300***' provides a standardised ***vocabulary*** for ISO standards coming under the umbrella title 'Security and Resilience' - which includes ISOs 22301:2019 and 22313:2020 - amongst others

The author / owner of this CRPM Part 3 guideline document (you are reading Vol 1 of the latter right now) is of the informed opinion (subjectivity acknowledged) that the usefulness and / or extent of much of such (ISO 23000) ***vocabulary*** falls significantly short of what is required

However (and the reason for including the last 3 paras above herein) - Clause 3 of ISO 22301:2019 introduced a further (***additional***) vocabulary - to be used 'over and above' (instead of / overrides) the ISO 23000 vocabulary (but ***only*** for the 31 terms listed in said clause 3 - otherwise the rest of the ISO 23000 vocabulary can be assumed to still apply)

If the reader is wondering why we have bothered to go to the trouble of including the last 4 paras above (in this CRPM Part 3 / Volume 1 document) - it is to draw attention to the ***significant inadequacy*** of **both** vocabularies in getting the meanings (of many [but not all] included words) across successfully, when used in a business continuity type context

As an example, take the fundamental (business continuity context) word '**activity**' and then take a look at the 3 definitions of 'activity' found starting on page 55

The first is our own (i.e. as produced by the author / owner of the document you are reading now). The second is the ISO 22301 version and the last comes from ISO 23000

Question: Which one does the reader think best explains what the word 'activity' actually means ***in the BC context***?

Answer: The author / owner etc. hopes that the reader agrees with him that the first definition does the job reasonably well - whilst the ISO 22301 version is rather hopeless - and the ISO 23000 version just a little less hopeless!

Accordingly, different (but equivalent in meaning) vocabulary is used herein (if thought to be clearer / more helpful than that found in the current ISO 23000 and 22301 versions)

This situation will be kept under regular review as (if) the latter 2 documents 'mature' with time to become something 'more useful' to interested readers (but don't hold your breath for this to happen anytime soon!)

Readers / users should account for all of the above when reading and interpreting terminology etc. (vocabulary) used in both Volumes of this CRPM Part 3

Deliberately Blank

Glossary / Vocabulary etc. (Know the' Jargon')

- With regard to ***Business Continuity*** (BC) related / specific ***terminology*** - there has * never been a really ***meaningful*** effort (by ISO or anyone else) to clearly, concisely and consistently provide a BC related glossary which 'does what it says on the tin / can'

  * *That said, due credit is given to certain organisations [i.e. **not** ISO] which **had** made some progress on this **in the past** - in at least better explaining (but still not being able to universally standardise) much of the BCMS related terminology in use. Some of that work is reflected herein*

  For example, take the 3 definitions of '***activity***' shown (starting) on the next page

  If you were training / studying to become a BC practitioner (or had some equivalent interest in the subject) - which of the 3 definitions / explanations shown (on the next page) conveys best the meaning of the word 'activity' - ***AS USED in the BC CONTEXT***?

  Choice of the correct answer is a 'no-brainer' of course - hope you got it right!

  For the associated rationale, see again the associated information provided (this document) under the heading 'Vocabulary (Glossary) - page 52

- Similarly, some inclusion of slightly ***differing*** explanations for the ***same*** term / definition has been made in this glossary (in quite a few places) - aimed at achieving a 'better understanding' of the associated meaning

- Where a definition required 'expanding' in order to further achieve better understanding - this was accomplished by means of using '***additional explanatory material***'. You will know when you find such a definition as it will be considerably longer than its 'normal' equivalent version

- It is anticipated that this CRPM Part 3 guideline will transition exclusively to *ISO 22300* terminology - when the latter has reached an appropriate stage of maturity, 'completeness' and standardisation in actual widespread, international use - i.e. at some future time (but again, don't hold your breath for this to happen anytime soon!)

Note 1 - users / readers might find difficulty in fully understanding what is written in this CRPM Part 3 (2 volume) guideline unless the following glossary is both studied ***and*** understood

Note 2 - 'Audit procedure' in detail is generally beyond the scope of this guideline. Consequently, audit-related / specific definitions are typically not included in this glossary. However, do note that (separate document) Volume 2 of this CRPM Part 3 guideline ***does*** provide some limited 'audit procedure' information - primarily for the purposes of establishing 'context' - where so needed

Note 3 - this glossary is always capable of improvement (especially for those for whom 'English' is not a first language) - and all suggestions / proposals for such will be gratefully received by the author / owner of this guideline document (via email please) at: ***info@aviation-erp.com***

- **Activity**

Processes undertaken by an organisation (and / or on its behalf) which are necessary to deliver and / or otherwise support (directly and / or indirectly) said organisation's individual and / or combined '**KEY product**(s) / **services** / **operations** / **tasks**' etc.

Key ***main*** activities are those whose failure might ***most quickly*** 'threaten' the viability of the associated (parent) ***key*** product(s), service(s) etc.

In an aviation context, they (key main activities) are typically carried out by e.g. ICT services; call / contact (reservations & customer services) centres; operations control centres; fuelling facilities; flight crew & cabin crew services; airport baggage systems; airport / airline freight systems; air traffic services; airport fire and rescue services; terminal and ground handling services; aircraft & airport engineering services; safety and security services etc.

Key ***supporting*** activities are those whose failure might threaten (in varying [generally 'less-urgent]' timescales) the associated (parent) key main activity / activities. In aviation again, key supporting activities typically include in-flight catering; HR, finance, legal & insurance services; facilities & procurement services; medical services etc.

'***Activities***' (and thus the organisation's departments / business units etc. which carry them out) generally 'do what they do' via implementation of associated **processes**

A particular process can extend (end [input] to end [output]) across several departments / business units - and can be internal and / or external to the organisation e.g. the aircraft refuelling ***process***; the aircraft parking ***process***; the airport check-in ***process*** etc.

Processes are often inter-dependent with / on other processes. They also require the '***support***' provided by ***resources*** (particularly people) in order to function

Activities are typically provided as a mix of those conducted directly by an organisation itself (e.g. airlines and airports) - and those depending on independent, third party suppliers / providers (e.g. ground handlers; fuelling services; CIQ; call centres etc.)

An organisation's activities (+ everything that they depend on as per above) provide the major ***inputs*** for the 2 fundamental aspects of facilitating the management of business continuity i.e.

- **'Risk Assessment'** *and*
- **'Business Impact Analysis'**

Known in common BC terminology as '***UNDERSTANDING the ORGANISATION***'

(See also definition of '***Procedure***')

…… *& another version* (taken from ISO 22301:2019)

Set of one or more (input) tasks with a defined output

…… *& another version* (taken from ISO23000:2018)

Process / set of processes undertaken by an organisation (or on its behalf) which produces or supports one or more of its products or services. For example, Accounts; Call-centre; ICT; Manufacture; Distribution

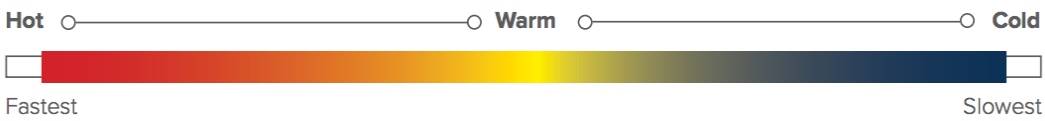
- **Alternate** (Recovery / Back-up / Fall-back) **Facility** / Site

  An organisation's designated **secondary / back-up** facility / facilities, held in a pre-determined state of readiness, in order to be able to take over designated operations / services / activities etc. from the organisation's associated ***primary*** facility / facilities - when necessary e.g. an associated disruptive incident rendering the primary facility / facilities unavailable for a 'significant period' (latter as defined by organisation itself)

  A ***COLD*** alternate facility typically requires equipping, set-up, manning etc. (but in extremis might require building from the ground up). Associated time period to get fully operational is typically in the timescale of days to weeks - possibly much longer. (Cheapest of the alternate options)

  A ***HOT*** alternate facility is typically fully equipped and set-up functionally - simply requiring manning (if not already manned) to make it fully operational. Associated time period to get fully operational is typically in the timescale of minutes to hours. (Second most expensive of the alternate options)

  A ***WARM*** alternate facility sits somewhere between the cold and hot versions described above. Associated time period to get fully operational is typically in the timescale of hours to days. (Third most expensive of the alternate options)



  A ***MIRRORED*** facility runs (in real time) identical processes etc. to the primary facility i.e. in most (if not all aspects) it is 'ready to go' very, very quickly. Users typically include certain types of ICT organisations, some elements of 'life-critical' operations, some military / security type ops etc. (The most expensive option)

- **Asset**

  Anything valued by an organisation - 'anything' including human, material, information, financial, reputational etc. (Assets can be tangible and / or intangible)

- **Audit**

  Systematic, independent & documented process for obtaining and (objectively) evaluating audit evidence, in order to determine the extent to which associated / specified criteria have been fulfilled

  Note 1: An audit can be a (first party) ***internal*** audit or a (second / third party) ***external*** audit. Audits can be combined (i.e. relating to two or more disciplines) if so required and feasible

  Note 2: An internal audit is conducted (on itself) by the associated organisation (being audited) itself - and / or by an external party ***on behalf of*** said organisation

  Note 3: Definitions of "audit evidence" & "audit criteria" can be found in (separate document) ISO 19011 entitled 'Guidelines for Auditing Management Systems'. (To view an 'unofficial' copy of the 2018 version click **HERE**. If the link no longer works try an appropriate internet search)

  Note 4: The fundamental elements of an audit include the determination of the ***conformity*** of an identified entity (e.g. an organisation; a person; a physical object; etc.) according to a procedure carried out by persons independent of / not being 'responsible' for said identified entity

  Note 5: An ***internal*** audit can be for ***management review*** and other ***internal*** purposes and can form the basis for an organisation's ***declaration of conformity***. ***Independence*** can be demonstrated by the freedom from responsibility (of the auditor[s]) for the ***activity*** being audited

  External audits (i.e. second or third-party audits). The former are conducted by parties having a direct interest in the organisation e.g. customers OR by others on their behalf. Third-party audits are conducted by external, independent auditing organisations e.g. those providing certification/registration of conformity; government agencies etc.

- **Backlog**

  The effects on an organisation of an uncontrolled build-up of unfulfilled work / product / services etc. - which occurs as a consequence of an activity / process / resource etc. being temporarily unavailable and / or having a 'lower than normal' output

  Note: a backlog may become so severe that it cannot be adequately cleared using ***normal*** resources - i.e. a "***Backlog Trap***" occurs (i.e. the backlog ***itself*** is the cause of ***further*** / ***additional*** disruption [over and above the original disruption event])

- **Business** (as used in a business continuity context)

  The entire infrastructure, as associated with all aspects of preparing and delivering the final outputs (key products / services / operations etc.) of a particular organisation - regardless of the latter's type, (e.g. Government / Public, Commercial, Not-for-Profit etc.) size, location etc.

- **Business Continuity** (BC)

  The process of ensuring (to a required / stipulated degree and insofar as is possible) an organisation's ability / capability to continue delivering its key products, services, operations and tasks etc - to an acceptable, pre-defined level and within acceptable timeframes - ***following a significant, disruptive incident*** - caused by an associated risk being realised (NB: ***BC*** is a sub-component of ***'risk'***. Risk is a sub-component of ***'resilience'***)

- **Business Continuity Context**

  The identification and definition of external & internal factors to be accounted for by an organisation - when setting the scope and criteria related to producing a ***BC Policy statement*** - and also during on-going ***BCMS programme management***

- **Business Continuity Management** (BCM)

  The process (within an organisation) of implementing, training, exercising, managing, maintaining, evaluating, reviewing and continually improving BC in general and, in particular, any associated BCMS (or equivalent) put in place by said organisation

- **Business Continuity Management System** (BCMS)

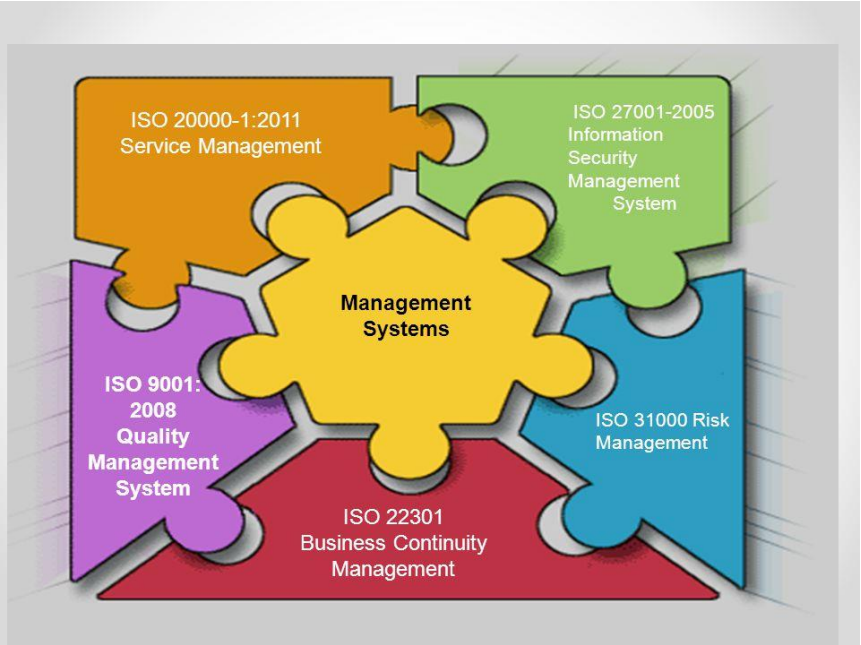
  That part of an organisation's overall '***modern*** management system' - which is applied specifically to all matters concerned with 'business continuity management'

  In common with all * modern management systems, a typical BCMS should include:

  - An ***organisational structure***
  - A BCM ***policy*** and ***objectives***
  - ***Management processes required to support*** the BCM policy
  - ***Competent*** (aware, trained, and exercised) ***people*** with pre-defined, documented & measurable BCM ***roles, responsibilities and accountabilities***

- ***Associated documentation*** / ***data*** e.g. plans, information, instruction, guidance, checklists, terms of reference etc. (also used to provide evidence as part of any audit / compliance process)
- An appropriate BCM ***infrastructure***
- ***Specific processes, procedures & plans*** required to support BCM
- ***Other required*** BCM ***resources*** - including budget, time, facilities etc.

* Examples of other ***modern*** management systems include 'quality'; 'environmental'; 'information security'; 'risk management'; 'energy' etc.



Note: the above diagram might be useful to better visualise some of the modern management systems in use today. However, do note that some of the associated 'years' shown (in the diagram) are incorrect e.g. ISO 9001 has been updated to a later year - as have ISOs 27001 and 20000-1 etc.

- **Business Continuity Objectives**

In the BC context there are three types of 'objectives' to consider and document i.e. strategic, tactical and operational. This definition refers to ***strategic*** BC objectives

BC ***Strategic*** Objectives

BC strategic objectives state / document the 'big picture' ***end purpose*** of what an organisation is aiming to achieve from the a business continuity context i.e. they apply to the organisation's BCMS as a whole. In order to check (on-going) that such objectives are being ***achieved***, they must be ***measurable***

Top management should ensure that:

- Information relating to the setting and achieving of strategic BC objectives is prepared, documented, reviewed and retained
- A statement is made and documented pertaining to how (in ***VERY*** general terms) the strategic BC objectives might be achieved / met

Strategic BC objectives should:

- Be consistent with the organisation's BC policy
- Be clearly stated
- Be relevant and specific
- Be achievable i.e. both actually and within (reasonable) time limits
- Be measurable
- Be monitored, reviewed and updated - as appropriate

Fictional examples of typical ***strategic*** BC objectives include:

- Implement /certificate (to ISO 22301 requirements) a BCMS system by (date)
- By (date) implement a BCMS which is; a) fully aligned with ISO 22313 guidance; b) adequately protects our key operations and; c) meets the requirements of our key stakeholders / customers
- Fully comply (by date) with all national business continuity legislation, regulation etc.
- Improve our ***tactical*** BC recovery time objectives (RTOs) by 50% within the next 12 months - whilst remaining within current budget constraints
- Reduce (over the next 2 years) our insurance premiums by 15% - as a result of introducing a BCMS fully compliant with ISO 22301 requirements

There are various methods of measuring achievement re the above e.g.

- Actual certification to the ISO 22301 standard is itself a measure
- Feedback from exercising (testing) is another type of measure
- If you do achieve the 15% reduction in insurance premium you actually ***have*** measured the success of the objective

For small to medium sized organisations (with no particular complexities) 'Strategic BC Objectives' are typically documented as an inclusive part of 'BC Policy'

Such objectives should be documented separately (i.e. in their own right) within BCMS documentation for the larger and / or more complex organisations - probably positioned just before / prior to the 'BCMS Policy' section

A suggested method of identifying strategic BC objectives might be to look at your own 'wish list' of ***BC Outcomes*** (see a little further below for some typical suggestions of the latter) and then conduct a 'brainstorming' session(s) with appropriate parties - to come up with what is required

Note that strategic BC objectives should be stated in general terms only i.e. brief, amalgamated / consolidated and to the point, as per the examples on previous page

As to who will be doing the brainstorming, the most likely candidates will be the BC Manager (or equivalent); the top management's 'BC champion' and any associated BC steering committee / similar. In certain types and / or sizes of organisation 'general workforce' representation is also likely

EXAMPLE: ***Wish-list of BC Outcomes***

Now might be a good time for the user / reader to become aware (in general terms at least) of what (according to ISO 22313) successful introduction of a BCMS into a typical medium to large sized organisation might have achieved when such project is 100% complete (i.e. what it should be producing in the way of what might be termed *'Desired **BC Outcomes**'*)

- ✓ ***Top-management fully 'on-board'*** - insofar as BC matters are concerned
- ✓ From BC viewpoint / context, the organisation's requirements ***to fully understand 'itself' internally*** - together with a similar understanding of the context & details of ***how it will need to interact and inter-relate with all appropriate external 'interested' parties*** - have been adequately researched, developed, documented, understood, accounted for, trained for, exercised for etc.
- ✓ ***Supply chain*** (if appropriate) adequately ***secured***
- ✓ A fully functional ***'incident response structure'*** is in place - ready to deal with the ***immediate*** consequences of whatever was the ***initial*** cause of a disruption, if appropriate (i.e. direct emergency / crisis response) - and to then go on to handle any associated (but separate) ***business continuity*** / ***business recovery*** type issues - as required
- ✓ etc.

- **Business Continuity Plan** (BCP)

  Documented processes, procedures, information etc. (consistent with associated 'BC Objectives, Policy, Strategy, Tactics' etc.) designed to guide an organisation in how to respond, resume, restore & recover ***to a pre-defined*** level of operation / service / output etc. - ***following a significant disruption*** event to one or more of its business activities

  Note - it is ***very*** important to clearly understand that production of a BCP is ***just one*** *of other* (equally important) *required elements* - comprising in total (i.e. all elements) a 'Business Continuity Management System'

  .....*and another (more concise but not so clear) way of saying this:*

  Business continuity methodology components - produced as a documented plan

- **Business Continuity Policy**

  A 'Business Continuity Policy' statement typically sets out the organisation's higher level view of the 'who, what, where, when, why, how' etc. type questions (and other relevant matters) associated with the establishment, day to day running and review of its own BCMS. For example:

  - Top management commitment to BC in general and financing / establishment / operation / maintenance / support etc. of a BCMS in particular
  - How BC objectives are to be proposed, approved, reviewed, measured etc.
  - Scope / type (strategic direction compatible, complexity, size, purpose etc.) of BCMS to be chosen
  - How, when and in what way(s) the BCMS should be delivered
  - Definition and documentation of key BCMS roles & responsibilities
  - How requirements of 'interested parties/stakeholders' might be met
  - Communicating 'the BC Policy' internally and externally

    BCMS governance / review - including commitment to 'continual improvement'
  - Review / update of 'the BC Policy'

- **Business Continuity Programme Management**

  An on-going (cyclical) governance & management process (supported by an organisation's top management & appropriately resourced) intended to implement and maintain 'business continuity management' in order to sustain 'organisational resilience'

  For an excellent explanation of what is meant by the term 'organisational resilience' - follow the below link:

  https://www.thebci.org/news/what-is-organizational-resilience.html

- **Business Continuity *'Requirements / Resources'* Analysis**

  The process of collecting, documenting and analysing information re the ***resources required*** in order to potentially continue / resume an organisation's business activities (following an associated and significantly disruptive event), at a level commensurate with supporting said organisation's declared BC Policy, Objectives, Strategies and associated Tactical Treatments / Solutions

Deliberately Blank

- **Business Continuity Strategy**

Note - ISOs 22301 & 22313 has now replaced the term 'Business Continuity Strategy' with 'Business Continuity Strategy ***and Solutions***'. The word ('Solutions') refers herein to what is covered below under title '**Business Continuity** (Tactical) **Treatments** / Solutions / Controls etc.'

Appropriate, strategic (higher level / longer term) choices made by an organisation - to ensure (insofar as is possible / practicable / desirable etc.) continued or resumed production / operation (typically following a temporary cessation of same) of its key product / services / operations / activities / tasks etc. (albeit to a potential, pre-defined [temporary] level of operations - typically [but not always] being ***below*** that of ***normal*** operations), following a significant, disruptive event

BC strategy is typically formulated (based) on the results of outputs from the associated '***understanding the organisation***' task

Very generally speaking, there are three 'generic' BC strategy options to be considered (i.e. choose the most appropriate strategy and expand upon it 'tactically') with regard to each key product / service / operation / activity / task etc. under consideration i.e.

1. Be ***fully*** productive / operational etc. - ***at all times*** (e.g. a trauma hospital)
2. Produce / Operate / Respond etc. to ***pre-defined*** (possibly incremental) and acceptable, ***minimum level***(s) (see definition of 'Minimum BC Objectives' - **MBCO**) within a pre-defined and acceptable ***time period(s)*** (see definitions of 'Maximum Tolerable Period of Disruption' - **MTPD** / and 'Recovery Time Objective' - **RTO**)
3. Do ***nothing*** (Pedantically speaking, the 'do nothing' choice is **not** a ***BC*** strategy. Rather, it is a ***RISK management*** strategy)

Note - within current BC terminology, there is a fairly common (and confusing) intermixed usage of the terms 'BC Strategy' and 'BC Options' (and probably some other such terms also?). Both terms typically refer to the same subject area - as defined above. However, only the term 'BC strategy' has been used in ***this*** guideline document

- **Business Continuity** (Tactical) **Treatments** / Solutions / Controls etc.

Tactical (general & operational level / shorter to medium term) measures, taken by an organisation, in order to achieve the requirements of an associated BC Strategy - with regard to maintaining continuity (to a ***pre***-specified minimum level) of ***pre-specified*** key product(s) / service(s) / operation(s) / activity (activities) / task(s) etc.

  - For maintenance of ***'Full Production / Operation'*** BC '***strategy 1***' above stipulates implementation of (typically [but not always]) pre-assigned and appropriate BC ***'tactical treatments*** / solutions' etc. (+ the associated resources) - commensurate with **immediate** (or as near immediate as possible [re the actual disruption circumstances 'on the day']) resumption / production / operation of the associated key product / service / operation / activity / task

Examples of 'what might need to be (near) immediately resumed' include:

- Surgical operating theatres
- Other critical hospital facilities
- Critical (blue light) emergency services
- Key main activity (and / or associated critical dependency) which can only be operated via associated ICT resources (e.g. single, unbacked website of an 'on-line only' retail organisation)
- An airline's only 24H call (reservations) centre - with no alternative power (electricity etc.) supply and / or no ICT backup capability
- A category IIIB (3B) Instrument Landing System (ILS) at an airport which occasionally experiences 'below ***normal*** limits' weather
- Critical Air Traffic Control facilities etc.

All such tactical treatments / solutions / controls etc. must be ready (as required) for near immediate implementation / application as required. This is typically achieved via a '**HOT**' system - possibly excepting e.g. critical ICT type services where a '**mirrored**' system might be more appropriate. Not forgetting the need for 'competent' people to immediately take over operation of such hot etc. backup facility - however this might be achieved

- For ***BC Strategy 2*** (see previous page), appropriate BC *'tactical treatments / solutions / controls* etc.' are applied in order to deliver what is required / specified. Some typical examples include (list is ***not*** exhaustive):

  - An appropriately equipped / resourced and located 'back-up / alternate' facility (**WARM** or possibly **COLD** [depending on what the related BC Strategy actually stipulates]) - where staff delivering key operations / services / activities - can be transferred, accommodated and operate in the required timeframes

  - Alternative suppliers and / or the 'self-storage (thus rapid availability) of identified stock and similar

  - Use of (competent / available) alternate staff to fill 'empty' posts

  - 'Working from home'

  - Reciprocal (mutual) aid arrangements with similar organisation(s) - at appropriate locations etc.

- *'**Do Nothing'*** (***BC Strategy 3*** - see previous page) ***might*** be regarded as an acceptable BC *'tactical treatment / solution etc.'* in ***appropriate*** circumstances

  For example, it is typically used following a ***cost*** / ***benefits analysis*** of the BC treatment(s) etc. available to meet a specified BC strategy - where the conclusion is reached that the potential benefit(s) (of doing something) would (or probably would) be outweighed by the associated costs / time / effort etc.

Note that there may be potential ***adverse*** implications in 'doing nothing' - if not managed correctly. Such implications typically affect brand, image & reputation type issues; crisis communications; financial considerations etc.

Consequently, in choosing the 'do nothing' BC strategy it is important to identify any further (knock-on) potential, ***adverse*** impacts which might arise as a result - and ***pre***-establish appropriate counter-measures accordingly

For example, the need to communicate with stakeholders / other interested parties as to 'why the decision to do nothing' was taken; providing some form of compensation or similar to those disadvantaged as a result of 'doing nothing' (e.g. airline customers) etc.

Note 1 - 'doing nothing' is a good example of a BC tactical treatment / solution etc. - which itself can potentially create further risks and associated adverse impacts - leading in turn to the need for further risk and / or BC tactical treatments / solutions.....and so on

Note 2 - the term ***'BC tactical treatment*** / solution / control' etc. is specific to ***this*** CRPM Part 3 guideline document only. Within (other) general BC terminology in use around the world it may also be known as e.g. '**BC Options**'; '**BC Tactical Responses**' etc. Even more confusingly, '*BC Options*' is also sometimes used to ***mean the same thing*** as '*BC Strategy*'!!!

BC tactical treatments / solutions etc. are ***unlikely*** to be applied in isolation - rather, a combination of the most appropriate treatments / solutions etc. will typically be applied. For example, an important (key) activity such as an ***airline's*** main operations control centre or an ***airport's*** terminal building management centre - will require consideration of some / all of the following (the list is ***not*** exhaustive):

- Use of a ***fully equipped, relatively nearby*** (i.e. a different location) ***& ready to go*** (WARM) ***alternative*** / ***backup facility*** (in this particular example the importance of rapid resumption of related services would be high - but probably not 'high enough' to go to the very considerable expense and 'complications' associated with operation of a HOT site (instead of a WARM site)
- A suitable system for ***rapidly reinforcing / replacing on-duty staff***
- A robust method of ***back-up communications*** (e.g. satellite phones, tetra radio [with telephone & messaging capability], smart phones with social media, human messenger etc.)
- Access to a back-up (off-site) but easily and relatively quickly accessible ***repository for important information*** *(hard copy)* ***and data*** *(soft copy / electronic info)*
- ***Use of cross-trained staff*** operating in appropriate secondary roles
- '***Working from home***' capability for selected staff
- etc.

- **Business Impact Analysis** (BIA)

  BIA (taken together with the ***other*** three components of the ***'understanding the organisation'*** task [see page 98]) is the foundation of ***Business Continuity Programme Management*** (BCPM). In very brief summary it (BIA):

  - Identifies an organisation's ***key product***(s) / ***services*** / ***operations*** etc.
  - Identifies ***key*** **main** ***activities and resources*** (internal & external) associated with delivering the above key product(s) / services / operations etc.
  - Identifies ***key*** **supporting** ***activities and resources*** (internal & external) associated with supporting delivery of the above key **main** activities etc.
  - Assesses the ***prioritisation*** (scoring by degree of urgency) of 'key *main* & key *supporting* activities' to the organisation, ***with regard to their continuity / resumption***, following a significant disruption event .....and
  - Assesses the ***impact over time*** of (uncontrolled & non-specific) disruption of such key main & supporting activities - on the delivery of the organisation's key products / services / operations etc. .....and
  - Estimates the timescales (***MTPD*** and ***RTO***) by which BC tactical treatments / solutions for each key main activity and key supporting activity above (individually - ***and*** in relation to each other where appropriate) must be applied, in order to avoid unacceptable consequences to the organisation and its stakeholders .....and
  - Identifies internal & external ***dependencies*** etc. - relating to the same 'key main activities' and 'key supporting activities' and, where appropriate, ***adjusts initial RTOs*** (as calculated above) to adequately account for same .....and
  - Sets the minimum level of business continuity operation (***MBCO***) to be achieved when a disrupted activity 'resumes' within or by RTO .....and
  - Identifies '***single points of failure***' for any further action.....and
  - Uses 'degree / level of adverse impact ***OUTPUTS***' from all / any of above as ***one*** of the ***INPUTS*** to the associated ***RISK ASSESSMENT*** process.....and

- ***Pulls together & documents*** the results of **ALL** of the above (and more) into a report which, when approved by top management, is used (going forward in the BCPM task) to formulate an associated '***BC Strategy*** / *Strategies*' and associated ***BC*** (tactical) ***treatments / solutions***

  The latter will, in turn, outline what the organisation then needs to achieve / provide / resource etc. - in order to try to ensure continuity of its key activities, following a significant disruption event to same .....and

- Identifies and accounts for ***other*** activities which ***might*** also require similar consideration from a business continuity context - but which are ***not*** expected to require application of the formal BIA & Risk Assessment etc. processes described above

  Note - known / expected seasonal factors e.g. peak trading periods; peak vacation periods for staff; deadlines for submission of legal, regulatory, financial and similar returns / reports etc. must also be factored into appropriate elements of all of the above - where appropriate

In summary, the BIA necessarily focuses on those activities - failure of which would ***most quickly*** threaten whatever it is that needs to be operated / produced / delivered by the organisation. This focus is typically directed to 'operational / high profile / high profit / up-front etc.' activities (i.e. key ***main*** activities - both internal and external)

However, many (if not most) of such activities will depend, in turn, on other 'backroom' activities (i.e. key ***supporting*** activities - both internal and external) which must also be similarly documented and analysed via the BIA

The BIA can be difficult to perform competently but must be 'got right' if it is to be effective. It can also take quite a long time - depending on the size and / or complexity of the organisation, the scope of the BIA, the co-operation of participants and the competence / experience / availability of the person(s) undertaking the associated data gathering & analysis of same - and, lastly, the degree of top management support

IMPORTANT NOTE

For ISO 22301:2019 a relatively '*new*' BIA related term / concept ('**Impact Categories**') was introduced

Whilst this subject has / had already been adequately addressed in (the separate) ***Volume 2*** of this CRPM Part 3 guideline document - associated 'additional explanatory material' can ***also*** be found herein (see Appendix C - page 113)

- **Business Recovery / Business Recovery Plan**

  Whilst Business Continuity is targeted (following a disruptive event) at operating an organisation's activities etc. ***to a pre-targeted minimum level of output*** (see MBCO) - ***within pre-targeted timeframes*** (see MTPD & RTO respectively) - **Business Recovery** aims thereafter to gradually ***restore*** such activities etc. to a more sustainable level than that required by MBCO - and eventually to 'normal operation' levels

  Note - Business ***Recovery*** *is outside the scope* of the CRPM Part 3 guideline document. Where mentioned herein - it is typically for contextual and / or information purposes only

- **Competence**

  The demonstrated ability of someone to adequately apply the knowledge, skills, experience etc. - considered necessary to achieve intended results / goals / targets etc. Competence is achieved via a mix of training, exercising, on the job experience etc.

- **Compliance**

  Fulfilment of a requirement

  When a 'requirement' is of a mandatory nature, the word ***conformity*** is sometimes used instead of 'compliance'. (Note that 'conformity' is an integral component of a 'modern management system' e.g. BCMS)

  (A ***Requirement*** / Need / Expectation etc. - can be stated, specified, implied, obligatory etc.)

- **Consequence** (See definition of 'Impact' + appendix C - page 113 '*Impact Categories*')

- **Continual Improvement**

  A recurring activity which incrementally enhances performance

- **Corporate Governance** (Governance, Risk & Compliance - [GRC])

  Companies generally direct & control their affairs by using a system of corporate governance - with 'Boards of Directors' (or equivalents) typically exercising such governance

  Responsibilities of the 'board' include setting strategic goals, providing leadership to put the latter into effect, supervising management of the business and reporting to stockholders on the board's 'stewardship'. The board's actions are typically subject to laws, regulations, rules, morals and the wishes of stockholders / shareholders.

The stockholder / shareholder role in such governance is to ensure that an appropriate (governance) structure is in place + appointment of suitable directors, auditors etc.

From a BC / Risk Management viewpoint, corporate governance generally includes a requirement to describe business risks to the organisation, via audited annual reports - together with the appropriate management / mitigation measures put in place to control such risks

In some jurisdictions a board level director assumes responsibility for the organisation's risk management *(**including BC**)* oversight responsibilities

- **Corrective Action**

  Action(s) taken to eliminate the cause(s) of non-conformity - and to prevent recurrence (See also '***Preventive*** Action')

- **Critically Time-sensitive & Critical Activities + associated Resources & Dependencies**
  (See also - 'Prioritised [Critical / Critically Time-sensitive] Activity')

  Component ***activities*** (+ their associated processes, procedures, resources, dependencies, inter-dependencies etc.) of an organisation's specified key product / service / operation etc. - which, if interrupted for a long enough ***duration*** (significant ***time*** / ***period***), might cause the associated organisation to incur unacceptably adverse economic / operational / reputational etc. impacts

  IMPORTANT NOTE - the term '***critical***' *(other similar terms used in BC = **'essential', 'high importance', 'urgent'** etc.)* as used herein - is typically used in the context of '***TIME***-criticality' - as per the two definitions immediately above

  However, it should ***also*** be interpreted (where appropriate) in a ***different context*** i.e. being critical for the purposes of prevention of death and / or injury + similar type impact event / situation - where ***time*** might ***not*** be the ***most*** significant factor. In which case (and for the purposes of differentiation) the term, 'critically time sensitive' might be replaced with just 'critical'

- **Dependency**

  Relates to how one activity may depend (for its functionality etc.) on a ***different*** activity. ***Inter***-dependency refers to the same concept - but now where all activities considered (being ***more*** than ***two***) depend on each other for functionality etc.

Disaster Recovery (DR)

The term '[Disaster Recovery]' describes the activities, processes and resources dedicated to prevention of an **ICT** type failure / significant disruption and, if such prevention proves to be unsuccessful - the application of the appropriate recovery technique(s) to eventually restore 'normal (ICT type) operations'

The term is today much misunderstood and misused - especially outside its ICT context. Use of this term in ***this*** guideline document will **ONLY** be as described above

Similarly, the term 'business continuity' is often (mistakenly) used today - where 'disaster recovery' would (at least pedantically) be the more appropriate term to use

- **Disruption** (Outage)

  One definition

  Anticipated and unanticipated events which significantly (and typically adversely) disrupt an organisation's normal business activities

  ..... & another

  Anticipated or unanticipated event leading to unplanned (typically) negative deviation(s) (from an organisation's objectives) with regard to the expected delivery of some / all of its (the organisation's) products and services etc.

- **Disruption Support Unit** (DSU)

  See (separate document) CRPM Part 3 / Volume 2 - pages 100 to 104

- **Documented Information**

  Information (including the medium on which it is contained / carried) which (if mandatory or otherwise binding) is to be controlled and maintained by the organisation which is 'responsible for it. Such information can be in any format and media - and from any source. It includes e.g.

  - Specific management systems (e.g. a BCMS) and their related processes
  - Info created in order for the organisation to operate (documentation)
  - Evidence of results achieved (records) etc.

- **Effectiveness**

  Extent to which planned activities are realised (i.e. occur / happen / take place etc.) - and planned results achieved

- **Emergency** (Emergency Response [Plan / Planning]) - (ERP)
- **Crisis** (Crisis Response [Plan / Planning])
- **Incident** (Incident Response [Plan / Planning])

All of the above terms can and do mean 'all things to all men' - depending on context, historical use, ignorance etc.

However, and as used in ***this*** (aviation related) guideline document, the terms '***emergency***' and '***crisis***' typically relate to some form of * ***very serious*** occurrence (e.g. a situation requiring urgent action to protect / sustain life; communicating and caring [and / or arrangement of same] with / for all those adversely impacted as a result of taking such urgent action etc.)

+ The initial (immediate / near-immediate / shorter term) response(s) to the above (e.g. evacuation; fire-fighting & rescue; immediate medical treatment; hospitalisation; provision of humanitarian assistance; provision of crisis related information etc. ***BUT*** - **NOT** THE APPLICATION OF BUSINESS CONTINUITY TYPE MEASURES)

* For an aviation context (as used herein) 'very serious' typically relates to a ***catastrophic aircraft accident type scenario*** or equivalent event

Consequences of such an emergency / crisis ***might*** (repeat - might) lead (in time) to activation of (separate) ***business continuity*** / recovery type ops i.e. **ADDITIONAL TO** (separate from but possibly running alongside) the emergency / crisis response itself

In other words, if the emergency / crisis response lasts long enough, it might need to be operated and managed ***concurrently*** with any eventual BC response (which can obviously cause major problems - particularly for organisation's having manpower / other required resources deficit)

As an example - a major aircraft accident might be termed an 'emergency' or 'crisis' - and the parent (or related) organisation's initial response typically guided by some type of ***emergency*** / ***crisis*** response plan (Note - '***Emergency*** **Response Plan** [**ERP**]' is the preferred term used in ***this*** CRPM Part 3 guideline document)

A greater or lesser degree of ***disruption*** might be associated with such an emergency (e.g. closure of the main airport / airport hub serving the [accident related] aircraft operator), requiring implementation of a ***separate*** business ***continuity*** plan and, eventually, a ***separate*** business ***recovery*** plan - for **BOTH** the accident airline (and its local reps e.g. a GHA) and airport concerned (as appropriate)

Note 1 - within ***BC 'common use terminology'***, **ALL** of the above named plans ('emergency', 'crisis' and 'incident') + supporting infrastructure are [**INCORRECTLY** & **CONFUSINGLY** ***from an aviation viewpoint***] 'lumped-in together' as an integral part of something known as an '**Incident Response Structure** - **IRS**' (see page 76)

The latter term (IRS) is used even though what is being responded to might, in fact, be a major emergency / crisis - (i.e. use here of the ***less impacting*** term *'**incident**'* [and '***incident** response plan*' etc.] in such circumstances will be potentially confusing ***if used in an*** **aviation** ***context*** - particularly as related to **flight operations**)

Note 2 - in **aviation** related terminology (particularly as related to ***flight operations*** again) the word '***incident***' typically refers to a ***MUCH LESS serious occurrence*** than that associated with the words '***emergency***' and '***crisis***'

'Incidents' happen relatively regularly within the aviation industry and are usually responded to in a relatively low key manner. They ***might*** give rise to consequences which require activation of associated (formal) business continuity plans and possibly (BUT ***very*** rarely) emergency / crisis response plans

Note 3 - **IMPORTANT** - for ***medium*** to ***larger*** sized airlines / airports / GHAs etc. (with adequate resources of the required type) - it is common for 'emergency / crisis response' ops and 'business continuity' ops to be **treated separately** i.e. ***separate*** plans; ***separate*** command & control systems, ***separate*** response teams (often) in ***separate*** locations; ***separate*** resources (to a degree) etc.

That said, a significant degree of co-ordination, co-operation and consistency between the two **must** obviously be applied - both during the associated planning, training and exercising phases of both - and during actual (real) operations *which might involve both operating **concurrently***

The ***exception*** to what is written just above might occur in the case of smaller / less well-resourced airlines / airports etc. - where the provision of manpower (in the context of providing adequate numbers of competent responders) and other resources might be problematic. The information referred to elsewhere herein (see page 43) provides some potential workarounds designed precisely for such a situation

Note 4 - Pulling all of the above together, it is vital for the reader / user to be 100% clear that (in the aviation industry - and for ***flight operations in particular***) it is common for the words '***emergency***' and '***crisis***' to be interchangeably used to a degree (typically with the same meaning i.e. that something pretty catastrophic is being referred to - more particularly, the mass casualty [aviation disaster] aircraft accident type situation)

Conversely, the average (medium to large sized) airline experiences aircraft ***incidents*** (of one type or another) on just about a daily basis. Typically they are ***low-key*** events and are responded to on most (but not all) occasions - almost as part of normal operations

Lastly, the consequences of an aviation related ***emergency*** / ***crisis*** might require concurrent or eventual application of business continuity measures. Same goes for the consequences of an aviation related ***incident***

- **Establishing the 'Context'**

  Defining, differentiating & documenting the external and internal parameters / factors (contexts) to be accounted for - when managing business continuity (and also when setting BC scope + criteria for the BC policy):

  External Context

  Typically includes:

  - The cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environments etc. - whether international, national, regional or local
  - Other external key drivers (influences) and trends having an impact on the objectives of the organisation
  - Relationships with (and perceptions and values of) external stakeholders / other external 'interested parties'

  Internal Context

  Typically includes:

  - Governance, organisational structure, roles and accountabilities
  - Policies & objectives - together with the strategies in place to achieve them
  - Capabilities, as understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies etc.)
  - Information systems / flows + decision making processes (formal & informal)
  - Relationships with + perceptions and values of internal stakeholders / interested parties
  - The organisation's culture
  - Standards, guidelines and models adopted by the organisation
  - Types and extent of contractual relationships

- **Evaluation**

  Systematic process of comparing measurement results with pre-stipulated criteria - in order to determine discrepancies between said criteria and said results

- **Gap Analysis**

  A survey aimed at identifying differences between 'what is required' - compared to 'what is actually in place'. In the context of this CRPM Part 3 guideline, the term / concept is typically applicable to an organisation's ***Business Continuity*** requirements

- **Hazard**

  See 'Threat'

- **Horizon Scan** (See appendix **B** to this document - starting on page 109)

- **Impact**

  One definition

  The (typically adverse) consequence(s) resulting from an inability (for whatever reason) to adequately undertake or fulfil a required business process or equivalent activity

  ..... & another

  The outcome (being typically [but not always] adverse) of a disruption type event - which affects an organisation's objectives

  Note 1 - such ***impacts*** might typically include (the list is not exhaustive) loss of life and / or injury; damage to the physical & social infrastructure of a community; damage to the environment; political, corporate or personal embarrassment; financial loss; breach of law / regulations / standards etc.; failure to achieve agreed service levels; increased costs of working; loss of competitive advantage; loss of credibility; loss of key skills; brand, image & reputation issues etc.

  Note 2 - See also the short article on 'Impact Categories & Weightings' - Appendix C page 113. Concept of the latter is used herein (and in the [separate] 'CRPM Part 3 - Volume 2') to **replace** the traditional RM and BC definitions / concepts of the word '***consequences***'

- **Incident**

  Event that can be (or could lead to) a disruption, loss, emergency or crisis

  IMPORTANT NOTE

  - For the purposes of aviation related operations (particularly flight operations) the above definition has been provided for info and contextual purposes ***only***
  - For the purposes of aviation related operations (particularly flight operations) the International Civil Aviation Organisation (ICAO) definition of '***incident***' shall apply herein (i.e. throughout this CRPM Part 3 guideline document). The definition is reproduced below:

An occurrence, (other than an aircraft accident)**, associated with the operation of an aircraft - which affects or could affect the SAFETY of such operation**

- **Incident Response Structure** (IRS)

See again info found on pages 72 & 73 with regards to the info starting just below:

IMPORTANT

'**Incident Response Structure**' is an 'official' ***BC*** term which is, unfortunately, subject to significant misinterpretation / confusion - **particularly if used in an *AVIATION* context** - where the term '***incident***' is specifically & internationally (ICAO) defined (and is typically **NOT *directly*** related to BC Ops whatsoever)

The intended meaning of 'Incident Response Structure' **in the BC context** includes **ALL** of:

- The **initial & on-going operational response** to 'whatever it was' that **also** (sooner or later) **might** cause associated disruption to operations (e.g. a catastrophic aircraft accident 'on-airport' - together with activation of associated **emergency / crisis response plans** [but **not** {i.e. at least not yet} **business continuity plans**])..... **PLUS (+)**
- Application of associated business **continuity** measures where required..... **PLUS (+)**
- Application of associated business **recovery** measures where required..... **PLUS (+)**
- Any other consequential response required e.g. 'humanitarian / welfare assistance' measures'; communicating with the media and other stakeholders (crisis communications) etc.

However, the above BC meaning is 100% **INAPPROPRIATE** for **aviation** (and even more particularly for **flight operations**) - as **emergency / crisis response** (as per first bullet point further above) is a **totally different discipline** (from BC) **in its own right** and (generally speaking) does **NOT** consider **business continuity** matters, excepting those required to support its **own**, specific functioning during **actual** emergency / crisis response operations (e.g. ensuring that water supply to responding fire and rescue crews [e.g. at an aircraft accident site] is maintained)

Similar applies when considering aviation related (particularly flight ops) **incidents**

In the aviation context the info shown in the 4 bullet points on the previous page (which, taken together in the ***BC context***, comprise the '**incident response structure**') **WOULD TYPICALLY *NOT* BE RECOGNISED**

Instead, the items covered in the first and fourth such bullet points would typically be known by airlines as the **ERP** ('emergency response plan' or similar term e.g. 'crisis response plan') - and by airports as the **AEP** ('airport emergency plan' or similar term)

The items covered by the second and third bullet points would simply be known as the '**business continuity plan** - **BCP**' and would typically **NOT** be a direct part of any emergency / crisis response operation (including associated pre-planning; training etc.)

Aviation related **ERPs** / **AEPs** etc. are **100% different** from aviation related **BCPs** - typically having * **different** command & control systems; operating from * **different** facilities with * **different** responding teams; * **different** documentation / checklists; * **different** resources etc.

* **NB**: See again associated info on pages 72 and 73 for further clarity (if required)

It is suggested that a more appropriate term for 'Incident Response Structure' (as used in a BC context) might be something like '***Contingency*** Response Structure' or similar.

However, as the former term was (as at 2020) still in widespread use *in the BC context*, **it *HAS* been retained in this guideline document** (i.e. the one you are now reading)

Nevertheless, the '**aviation**' (particularly flight operations related) type user / reader **must** always keep in mind what is written above (and also on pages 72 and 73) when emergency / crisis response ops (particularly flight operations related) are being conducted and there is the possibility of associated and concurrent BC ops also being conducted (e.g. typically as a 'knock-on' consequence of the ***initial*** emergency / crisis response operation itself)

- (Other) **Interested Party / Parties** / Considerations

  A person, group of persons, organisation(s) (and even 'something' in certain circumstances) who / which can affect **AND / OR** be affected by (actually or perceptually) - a decision and or an activity and/or a mistake and/or neglect etc.

  (Examples of 'other interested parties' include **1**: customers / clients, owners, employees / personnel, shareholders/ financial investors, providers / suppliers, banks, insurers, governments, regulators, auditors, unions, partners, societies, professional bodies etc. Less obvious examples include **2**: competitors, the community / local population [permanent & transitory], the organisation's operating environment, the media, protest / pressure groups etc.)

  Note - the intent is to include **all** elements having an interest(s) in an organisation and vice versa e.g. those listed in **1** above typically fall under the concept of '***stakeholders***' - whereas those listed at **2** may not be stakeholders but may ***still*** have an interest of one form or another

- **Key** (Prioritised) **Product / Service / Operation / Task** etc. (See definition of *'**Activity**'*)

  What an organisation is primarily all about i.e. what it 'does'

  For example and for an **aircraft** operator - key (prioritised) services / operations might include the transport of passengers by air; the transport of cargo and similar by air; the provision of associated leisure services (vacations, hotel & car hire bookings etc.); provision of search & rescue services by air; fire-fighting operations by air…… and so on

  For an **airport** operator - key etc. services / operations might include providing passenger and cargo services to aircraft operators; provision of air traffic control services; provision of fire-fighting and rescue services; provision of refuelling services: provision of 'duty-free services etc.

  Significant disruption to an organisation's key product / services / operations etc. – which lasts for a ***significant*** time / period / duration, might have unacceptable (adverse) impacts on the organisation and / or its stakeholders / other interested parties

  Note 1 - the term '***significant***' should be defined by the organisation - as it will typically vary for different types of product / service / operation. **Note 2** - in addition to appearing anywhere else, 'key product / services / operations' should also be documented within the *'**scope**'* section of an organisation's '**BC Policy**' statement. **Note 3** - see also definition of 'product / service'

- **Management System** (e.g. a 'Business Continuity' Management System [BCMS])

  One definition

  Set of interrelated / interacting elements, measures etc. produced by an organisation (having been researched / designed / developed etc. to establish related policies, strategies, plans, processes, resources, competencies etc.) required to achieve pre-defined objectives of benefit / worth / advantage etc. to said organisation

A management system typically comprises an organisation's structure, roles, responsibilities, plans, operations, performance, review and continual improvement - and can address subject matter areas individually and / or in combination

The scope of a management system can include e.g. an entire organisation, specific and identified functions of an organisation or one or more functions across a group of organisations

See also definition of a 'Business Continuity Management System' (BCMS)

..... & another

- *Modern* **Management System** (MMS)

ISO (International Organisations for Standards) ***management system standards*** (MSS) assist organisations to improve performance by specifying (generic) repeatable implementation steps necessary to achieve specified goals and objectives. They also help to create an organisational 'culture' engaging in a continuous cycle of self-evaluation, correction and improvement of specified operations and processes - via improved management leadership & commitment, increased employee awareness etc. Benefits include:

  - More efficient use of resources and improved financial performance
  - Improved risk management (and thus 'business continuity' too)
  - Better protection of people and the environment etc.
  - Increased capability to deliver consistent and improved services and products, thereby increasing value to customers and other stakeholders

MSS are the result of ongoing consensus amongst international experts in global management, leadership strategies and efficient / effective processes and practices - and can be implemented by any organisation conducting any type of operation. Some typical examples are ISO 9001, ISO 14001, ISO 50001, ISO 31000 and ISO 22301 - being formal, international 'standards' applying respectively to quality management, environmental management, energy management, risk management & business continuity management

One of the fundamental MSS principles is that included standards work together e.g. where an MSS is already in use in one part of a business and consideration is being given to implementing additional MSS' in other areas. This is accomplished via ISO's 'high-level structure' (HLS) i.e. management standards are structured in the ***same*** (general) way regardless of type of application e.g. users familiar with one particular MSS should then better understand the concepts and application etc. of another

Furthermore, ***some*** parts of any MSS (defined by ISO in something known as '**Annex L**') use identical terms, definitions and text. This improves coherence, recognition and simplification. It is also useful when operating a single 'integrated' management system i.e. meeting the requirements of two or more involved MSS' concurrently

A BCMS (as with all other 'modern' management systems) should:

- Include a Policy (with inclusive scope, objectives, exclusions etc.)
- Account for the need for competent people with defined responsibilities etc.
- Account for the need to produce BCMS *management processes* etc. relating to:
    - Scope, Policy, Objectives etc.
    - Planning
    - Implementation and Operation
    - Performance Assessment
    - Management Review
    - Continual Improvement
- Provide for associated documented information to be produced and maintained

Note 1 - The word '***modern***' (as used in '*modern* management system') was ***originally*** (i.e. in **2012**) included in the title of the above definition as, in that same year, ISO was in the process of introducing a new ('modern') form of management system which was distinct from its predecessors. The word is retained in this definition today for ***historical*** purposes only

Note 2 - A ***Type 'A'*** MSS (e.g. ISO 22301) contains ***requirements*** against which an organisation can claim conformance, whereas a ***Type 'B'*** does not i.e. only recommendations (***guidelines***) + supporting information are included in the latter. Some MSS contain a mix of requirements and guidelines - and (as they contain requirements) are still considered to be a Type 'A' MSS

A Type 'B' MSS (e.g. ISO 22313) typically provides guidance on implementation of its equivalent Type 'A' MSS (i.e. ISO 22301 in the case of ISO 22313). However, some Type 'B' MSS are independent in their own right

A 'TS' (Technical Specification) MSS typically provides additional, explanatory material with regards to an associated 'standard' type MSS e.g. the 5 'TS' documents listed in the top half of page 34 concern ISO 22313. Logically, all info provided in ISO 22313 related 'technical specifications' ***should be included in ISO 22313 itself***. The fact that it is not (and requires ***additional*** purchase from ISO of the 5 TS documents mentioned just above) says a lot about ISO's 'business model' with regards to 'making money' - obviously at the expense of its customers (see also Appendix E [starts page 132] of the document which you are reading now)

For more on MSS see: https://www.iso.org/management-system-standards.html

See also definitions of 'Business Continuity Management System' and 'Management System'

- **Maximum** (amount of) **Tolerable** *Data* **Loss** (MTDL)

The maximum loss of *data / information* (electronic & otherwise [e.g. hardcopy]) which an organisation is able to tolerate (see also 'Recovery Point Objective - RPO')

Note 1 - the 'age' of the lost data could make operational recovery difficult / impossible. **Note 2** - the value of the lost data could be substantial enough to put the associated organisation's business viability at risk. **Note 3** - the concept of MTDL **MUST** be clearly understood and incorporated into an associated BCMS. However, this CRPM Part 3 guideline document concentrates, in the main, ***only*** on MTPD (for more information see again 'scope' page 50)

- **Maximum Tolerable Period** of **Disruption** (MTPD) (Maximum Acceptable Outage - **MAO**)

(See also definitions of '***Activity***', '***Recovery Time Objective*** - *[RTO]*' & '***Minimum Business Continuity Objectives*** - *[MBCO]*')

Estimated period of ***time*** it would take for the consequences of an adverse impact(s), arising as a result (for whatever reason - but typically termed 'disruption / interruption') of **not** providing an organisation's **key** product(s) / service(s) / operation(s) / activities etc. - **to become unacceptable** to the organisation's (impacted) stakeholders / other interested parties

Overarching (strategic) MTPDs should be estimated, approved & documented for **EACH** of an organisation's **key** product(s) / service(s) / operation(s) / activity(ies) etc. -

.....followed by MTPD estimations for **each** associated (***subordinate***) key **main** activity etc. required to produce / operate etc. its (parent) key product / service / operation / activity etc. (as required)

Note - The estimation & allocation of MTPDs for ***key main activities*** **may**, in turn, require ***re-adjustment*** of the ***initially*** estimated ***strategic*** MTPDs referred to above

Further MTPDs should then be set, in turn, for **each** associated (***subordinate***) key **supporting** activity required to support its (parent) key **main** activity etc.

Note - The estimation & allocation of MTPDs for key **supporting** activities **may**, in turn, require ***re-adjustment*** of the ***initially*** estimated **key main activity** MTPDs referred to above

Many activities are dependent on the continued operation of external suppliers and similar. Accordingly, the organisation should make all reasonable effort to ensure that suppliers are not / do not become '**single points of failure**'

This can be achieved e.g.

- by use of appropriate 'service level agreements - SLA' within contracts
- by engaging more than one supplier to provide the same product / service
- by requesting suppliers to adopt their own BC measures / techniques - including the setting of MTPDs, RTOs, MBCOs etc. for their own key products, services, operations and activities

IMPORTANT

'***Subordinate***' MTPDs must be ***equal to or shorter*** (in terms of time period) ***than an associated***, '***parent***' ***MTPD***. This is why changes to a subordinate MTPD must then (always) be cross-checked with its parent MTPD - to see if a consequential / associated change in the latter is then required.....and so on

Note 1 - Most (if not all) 'activities' comprise a series of associated (subordinate) ***processes***. For the sake of brevity the latter have been ignored in what has been written above (previous page)

However, in reality, all such processes (as associated with their 'parent' activities) **must be similarly accounted for** - and any which are considered 'significant' from the business continuity viewpoint are to be assigned MTPDs in their own right. Such MTPDs must then be 'managed' if necessary - in a similar way to that documented on the previous page

Note 2 - Some typical 'consideration' factors used in estimating MTPDs include:

- Potential (adverse) ***impact(s)*** on staff / public well-being (humanitarian; welfare etc.)
- Potential (adverse) ***impact(s)*** re breaches of statutory and / or regulatory and / or 'best practice' (including any adopted standards) and / or similar requirements
- Potential ***damage*** to brand / image / reputation
- Potential financial ***damage***
- Potential ***deterioration*** of product / operational capabilities / service quality etc.
- Potential environmental ***damage***
- ***Other*** potential factors specific to / specified by the organisation

Note 3 - The term / words 'Maximum Tolerable Period of Disruption - MTPD' might be difficult to correlate with its/ their actual meaning, as given on the previous page - and significant debate has occurred (over recent years) concerning same. Such debate is beyond the scope of this guideline document - but suffice it to say that the alternative term '**Maximum Acceptable Outage** - **MAO**' is much preferred by the author / owner of this CRPM guideline document. The definition of MAO ***is the same*** as for MTPD

- **Measurement**

The process used to determine a 'value' - hence 'measurable' can only refer to something which has a value of some kind (Note - the word 'value' is not defined by ISO)

- **Minimum Business Continuity Objective**(s) (MBCO)

Pre-planned ***minimum*** / ***acceptable etc. delivery levels*** of an organisation's key product / services / operations etc. - together with (+) the latters' associated, subordinate activities etc. (all as related to various [potential] ***disruption*** scenarios) - ***predicted*** as being ***achievable*** by a ***pre-defined*** Recovery Time Objective(s) (RTO)

Note - '***pre-planned delivery levels***' etc. (as per definition above) are typically stated in terms of 'time-prioritisation e.g. '.....an MBCO of 25 % to be available **within *two hours***; 50 per cent **within *two days***; full (normal) service **within *one week*** etc.....' (See also Notes 1 & 2 which accompany the definition of '***Recovery Time Objective*** - ***RTO***')

- **Monitoring**

  Finding out (determining) the status of a system, process, product, service or activity. In order to 'determine status' it will typically be necessary to 'check, supervise and / or critically observe' etc.

- **Non-conformity**

  Non-fulfilment of a requirement

- **Objective**

  One definition

  The end purpose / aim of a process, of an activity, of an organisation as a whole etc. Objectives are typically expressed in terms of ***measurable*** targets

  ..... & another

  Result(s) to be achieved

  - Objectives can be strategic, tactical or operational and relate to different 'disciplines' (e.g. financial, health and safety, environmental, security, risk & business continuity etc.) and scopes (e.g. organisation-wide, department, business unit, project, product, process etc.)
  - Objectives can be expressed e.g. as an intended outcome, purpose, operational criterion - and by use of other words with similar meaning (e.g. aim, goal, target etc.)
  - Objectives must be measurable in some way, shape or form
  - (Where used in relation to a BCMS) - objectives are typically set by the organisation, with the goal of achieving pre-specified targets in pre-specified timescales (both being consistent with the organisation's business continuity ***policy***)

- **Organisation** (Entity)

  One definition (BC context)

  Any entity to which the concept / practice of business continuity actually and / or potentially applies / is applicable. The scope of this term (as used herein) typically refers to ***medium*** to ***large*** sized (and / or complex) entities - unless stated otherwise

  ..... & another

  Person or group of persons having his / her / its own functions - together with associated responsibilities, authorities and relationships etc. - necessary to achieve pre-defined (by the * person or group of persons) objectives

  * For example:

    - A sole-trader
    - A company, corporation, firm, enterprise
    - An authority
    - A partnership
    - A charity
    - An institution etc.

  For organisations comprising more than one operating unit, a single operating unit can be defined as an organisation in its own right, as required

- **Outsource**

  An arrangement made by an (originating) organisation with another (different) organisation - whereby the latter performs all or part of the former's functions, processes, services, activities etc.

  With regards to a particular, originating organisation's BCMS, the external organisation itself is outside the scope of said BCMS - **BUT** the outsourced function, process etc. ***is*** within said scope

- **Performance**

  A measurable result

  Performance relates to quantitative and qualitative results re the management of activities, processes, product, services, systems, organisations etc.

- **Policy**

  An organisation's intentions & direction - as formally expressed by its top management

- **Preventive Action**

  Action(s) taken (to try) to prevent a potentially, undesirable situation(s) from being realised (from occurring)

  Note 1 - ***preventive*** action is taken to **prevent occurrence** etc. - whereas ***corrective*** action is taken to **prevent recurrence / re-occurrence**

  Note 2 - The term (but not the concept / meaning of) ***preventive action*** went 'out of fashion' when ISOs 22301 / 22313 were first introduced in 2012. This was a mistake which the 2019 / 2020 versions respectively failed to correct. In ***this*** CRPM Part 3 document (you are reading Volume 1 of the latter right now) both the term and the concept are 'alive and well'!

- **Prioritised** (Critical / Critically Time-sensitive) **Activity**

  An activity / activities to which the necessary degree of urgency is given - so as to avoid unacceptably adverse impacts to an involved organisation - during any associated 'disruption' type event (see also 'Critically Time-sensitive & Critical Activities + associated Resources & Dependencies')

- **Procedure**

  A ***procedure*** (written or otherwise) is a specific way of carrying out an associated / parent '***process***' - typically comprising (at its simplest and in relation to the latter:

  - Who performs what action(s)
  - In what sequence the action(s) (+ the defined steps in the action[s]) occur(s)
  - The criteria (standard[s]) which must be met in performing the action(s)

  Documented procedures can be general, detailed or anywhere in between. Whilst a simple procedure might comprise e.g. just a simple flow diagram, a detailed procedure could be e.g. a one page form or it could be several pages (or many more) of text / flow and other diagrams / images etc.

  A procedure typically:

  - Defines and controls its ***associated*** (parent) ***process***
  - Explains how the above should be accomplished, who should do it, under what circumstances, when / how often etc.
  - States and reflects associated authorities, responsibilities, resources etc. - to be assigned / allocated / used
  - States which inputs should be used and what outputs should be delivered

- **Process**

An inter-related / inter-active operation - which uses ***resources*** (one or more of which will probably be a procedure) to transform ***inputs*** into ***outputs***. (Note - it is possible that the output from one process can become the input for another. Note also [simplistically speaking] that an organisation's departments / business units etc. typically use associated processes to perform their activities)

One should be able to ask the following typical questions (and get appropriate replies) when defining a typical 'work' related **process**:

'Activities' - **What** are the basic jobs carried out in your department / business unit?

'Inputs / Resources' - **What** inputs / resources do you need to do your work / jobs?

Where does 'what you need (to have) in order to do your work / jobs' - come from?

Can you explain (provide an overview of) **how** your 'work / job operations' function?

'Outputs' - **what** 'deliverables' result from your work / jobs?

Who receives the 'results' (deliverables) of your work / jobs?

How do you know if you've 'done your work / jobs correctly'?

For a simplistic example of a **process** - take 'making a cake'

The ***input*** comprises the cake ingredients; the ***output*** is the cake and the 'bit in the middle' uses ***resources*** such as the chef / cook, a recipe, utensils, crockery, a stove etc. - to transform the input into the output

Note - in this simple example the ***recipe*** would technically be termed a '***PROCEDURE***' - and what the chef does as **'Key Main Activities'**. There are no **'Key Supporting Activities'** in this particular process

Taking this example a little further - if the cake making process was a part of a 'cake-selling' outlet (e.g. the '***organisation'*** is a cake shop) - then 'cake making and selling' may be considered to be the '**KEY PRODUCT / SERVICE** etc.' of that organisation

- **Process Mapping**

  A process map is a 'tool' commonly used to ***visually*** illustrate (on paper; electronically etc.) work flows. It can also be used as a communication tool, a business planning tool and a tool to help manage an organisation. Key elements include:

  - Inputs
  - Outputs
  - Activity steps
  - Decision points
  - Functions

  Process mapping involves the gathering and organising of facts about the required work - and displaying them in a visual format so that they can be questioned and improved upon by 'knowledgeable' people. It also aids in understanding by 'abstracting' (i.e. using visual 'symbols' consistently) & by masking unnecessary detail

  The standard lines and symbols used on a process map *(not included here)* help us to record concise sentences for every step in the process - which tells the user / reader:

  - What is happening
  - Where is it happening
  - When is it happening and how long it will take
  - Who is doing it
  - What resources are required

  Process mapping is used to gain / improve 'better understanding' of a subject - and is typically used in the BC context - as part of the ***'Business Impact Analysis'*** (BIA) process

- **Product**, **Service** etc.

  Output / outcome provided by an organisation to interested parties e.g.

  - Aviation related services including passenger and cargo flights; tour operator type services, air traffic control ops, sale of duty free products at airports etc.
  - Manufactured items
  - Insurance / Banking / Finance etc.
  - Medical services e.g. Hospitals, Nursing etc.

- **Recovery**

  With regards to an 'affected' organisation - 'recovery' describes the (typically) ***incremental*** restoration of product / service etc. (eventually) to 'normal business' level(s) - following a significant 'disruption type event' to said product / service etc.

  (See also 'Recovery Point Objective [RPO] & Recovery Time Objective [RTO])

- **Recovery Point Objective** (RPO) (Critical Data Point)

  The **RPO** is the ***maximum acceptable level*** (to the organisation) of ***data / information*** loss following an associated disruption 'event' (e.g. disaster [natural or man-made], criminal act / terrorism, negligence, ICT, Fire / Flood etc.) which could cause such loss

  The **RPO** thus represents the ***point in time***, prior to such an event or incident occurring, to which lost data (electronic and / or hard copy) might be successfully recovered (provided that the most recent, planned backup copy [if any] etc. of the lost data is available 'somewhere')

  ..... *& another definition*

  The ***pre-planned target*** set for the status and availability of data (electronic and / or hard copy) at the start of a recovery process

  See also 'Maximum Tolerable Data Loss' (MTDL). **Note** - the general concept of RPO must be clearly understood. However, provision of an associated, detailed explanation of same is outside the scope of this CRPM Part 3 guideline

- **Recovery Time Objective** (RTO) - (RTO concept is typically that of a *'**prioritised timeframe**'*)

  A pre-determined target ***time*** set by an organisation for * resuming *key* **main** *activities* (and, consequently, the latters' [associated / subordinate] *key* **supporting** *activities* - where appropriate) to a pre-determined level of output (see MBCO) - following an associated, disruption type event

  (Reminder: In ascending order - *key* **supporting** *activities* relate to their associated [parent] *key* **main** *activities* - which relate in turn to their associated [parent] *key* **product**(s) / **service(s)** / **operation(s)** / **activities** etc.)

  Set RTO too late & the organisation could encounter big resumption problems. Set it too early & the associated costs of managing same might outweigh the benefits

  * The terms '***resuming***; ***resumption***' etc. should not necessarily be taken as being related to ***normal*** *(full)* delivery levels of a product, service or operation etc. - although the latter would still be the case in certain circumstances e.g. for a surgical operating theatre; for some emergency services & similar etc.

IMPORTANT

'***Subordinate***' RTOs must be ***equal*** to or ***shorter*** (in terms of time period) than an ***associated***, '***parent***' RTO

This is why any subsequent ***changes*** to a ***subordinate*** RTO(s) must then (always) be cross-checked with the specific, parent RTO - to see if a consequential / associated (knock-on) change in the latter is also then required.....and so on

Similarly - all '***top level*** (longest time duration) ***RTOs*** must fall within (be the same or earlier [equal to or shorter] in time) than their ***associated*** (parent) ***MTPD***(s)

This is why any subsequent changes to a ***top-level*** RTO(s) must then (always) be cross-checked with the ***specific*** parent MTPD - to see if a consequential / associated (knock-on) change in the latter is then required.....and so on

Note 1 - RTO calculations for a particular business activity may, in turn, be dependent on RTOs calculated for one or more ***OTHER*** business activities - and vice versa

For example, if activity **A** depends for its recovery upon activity **B**, then the latter's RTO must obviously be equal to or less (in terms of time) than that of activity **A**

If this is not so, the RTO for activity **B** must be adjusted (reduced) accordingly

Where it is not possible to adjust e.g. the latter RTO (for **B**) as described (for whatever reason) then an alternative, acceptable (to the organisation) solution must be found

Note 2 - If an RTO is changed for whatever reason - the ***associated*** (existing) ***MBCO*** must also be checked to see if it remains appropriate - with regard to such ***changed*** RTO. If no longer appropriate, the MBCO must be re-defined, approved and documented wherever so required

Note 3 - Most (if not all) 'activities' comprise a series of associated (subordinate) ***processes***. For the sake of brevity the latter have been ignored in what has been written above (previous page)

However, in reality, all such processes (as associated with their 'parent' activities) **must be similarly accounted for** - and any which are considered 'significant' from the business continuity viewpoint are to be assigned RTOs in their own right. Such RTOs must then be 'managed' if necessary - in a similar way to that documented on the previous page and above

- **Requirement**

  Need, expectation etc. which is stated, specified, generally implied, obligatory etc.

  (A specified requirement is one that is stated e.g. in documented information)

- **Resilience**

  The ability of an organisation, system, network, activity, process (etc.) to:

  - absorb the adverse impacts of an interruption, disruption, loss (etc.) to its products, services, activities (etc.) - *and*
  - continue to provide a minimum acceptable level of same within a desired (pre-planned) timescale (i.e. ***business continuity***) - *and*
  - return to 'normal ops' ASAP after that (i.e. ***business recovery*** / ***resumption***)

- **Resource**(s) (BC specific) (Continuity Resources)

  An organisation's assets (including e.g. people, skills, information [electronic and / or otherwise], technology [especially ICT], plant, equipment, premises, facilities, supplies etc.) - all being necessary (when required) in order to operate in general and meet its declared ***business continuity objectives*** in particular. Most organisations will need to use at least some resources which require ***external*** sourcing

- **Risk** (see also '***Threat***' and '***Vulnerabilities***')

  One definition

  Evaluation of a specified ***threat*** (+ any associated ***vulnerabilities*** re what it is that is being 'threatened') to / on something / someone (the latter being subject to that threat) - which, when combined with the ***impact*** of that threat (on that something / someone) should it actually occur (be realised) - corresponds to the ***risk*** (with regards to that something / someone) - as related to / in the context of / with regards to that specified threat

  By its very nature risk is neither precise nor scientific i.e. it is typically ***subjective***

  The considerations of any particular risk might (in appropriate circumstances) be influenced by any projected negative (adverse) & positive (beneficial) outcomes (see definition of 'Risk Appetite' re the latter outcomes) of potentially taking on that particular risk in the first place (assuming that there is a choice - sometimes there is not [e.g. a natural disaster occurrence])

  One (***but just one***) of several methods used to 'treat' (deal with) risk uses appropriate BC measures (via implementation of appropriate BC strategies & associated tactical solutions / treatments etc.)

  ..... *& another definition*

  Any internal or external situation / event having the ***potential*** to impact upon an organisation - which might (if it occurs) prevent the latter from successfully achieving some / all of its business objectives; capitalising on its opportunities etc.

  ..... *& another definition*

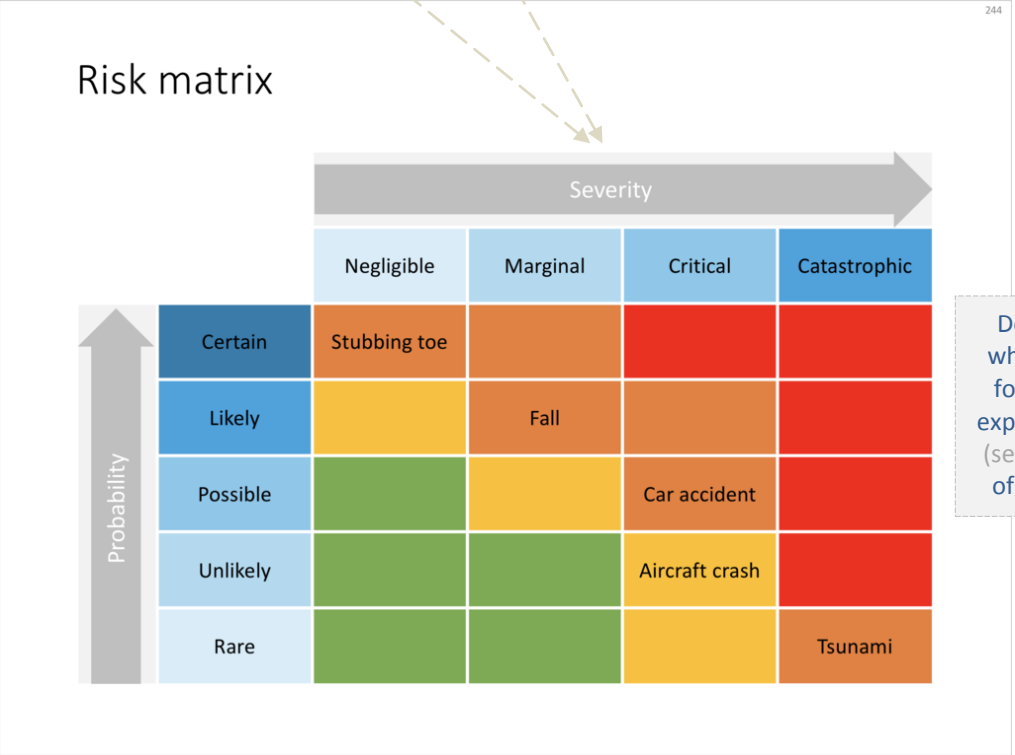
  Effect of uncertainty on objectives

  The term 'effect' relates here to some form of '***deviation from the expected***' - positive or negative

  The term 'uncertainty' refers here to how deficient (ranging from total to zero) is the degree / amount of information, data etc. available (relating to the understanding / knowledge etc. of a specified risk event [situation etc.] and its potential consequences, likelihood etc.) with regards to an organisation's specified objective(s)

Risk is often expressed in terms of the potential consequences / ***impacts*** (typically [but not always] negative / harmful etc.) of a specified event (should it occur) - ***combined with*** the associated ***probability*** (likelihood) of said event actually occurring

Note - in diagram below the word '***Severity***' has the same meaning / intent as the words '***consequences*** / ***impacts***' referred to in the above paragraph



Don't worry about what's in this matrix for now - all will be explained in Volume 2 (separate document) of this CRPM Part 3

- **Risk Analysis**

  Process to better understand the nature and estimated degree of identified risk to an organisation, together with the potential for consequent damage (adverse impact(s)) should such risk ever be realised (i.e. actually become a reality / occur)

  Risk analysis also forms the basis for '***risk evaluation***' and consequent '***risk treatments / controls***' - as required

- **Risk Appetite** (see also 'Risk Tolerance')

  The ***amount*** & ***type*** of risk that an organisation is broadly willing to pursue / retain (voluntarily accept / tolerate / be exposed to) ***at any particular point in time*** - with a view to attaining / maintaining / improving '***value***' (whatever the contextual term 'value' means to the organisation on a case by case basis) re its business objectives

The use of risk appetite typically depends upon the mission, culture, policy and other factors which determine 'what an organisation is' - how it goes about its business etc.

For example - **BC planning** is one (but ***only*** one) of several elements (treatments / controls etc.) of the ***Risk*** Management process, all such elements designed to try to ensure that an organisation can continue to deliver its key products, services etc. to clients / customers etc. - when set against potential threats - which might (if realised) adversely impact on such delivery

The depth of risk (including BC) planning and measures ***applied*** depends upon the level of risk on the organisation which it (has typically [but not always] already considered) is prepared to accept - i.e. ***as predicated on its declared & current risk appetite***

To develop this a little further with regards to the BC context, risk appetite can typically influence the organisation's choice of ***MTPD***, ***RTO*** and ***MBCO***. For example, the greater the risk appetite - the longer (relative / compared to the ***no*** / ***zero*** risk appetite situation) the RTO and MTPD timeframes might be **and** / **or** the lower the 'target level of continuity operations (MBCO / MAO) to be achieved by RTO'

For example, procurement / allocation (***or not***) of required resources (to operate e.g. a BCMS) will be influenced by risk appetite

- **Risk Assessment** (RA)

  Overall process of threat (and thus risk) identification + risk analysis + risk evaluation

  RA involves identifying internal and external threats & associated vulnerabilities (to the organisation); assessing the likelihood and impact of an event arising from such threats / vulnerabilities; identifying / defining critical functions necessary to continue operations should such threats be realised i.e. actually occur; identifying / defining / costing the controls necessary to reduce exposure to the threats & vulnerabilities

- **Risk Category**

  Similar risks can be grouped together in categories - e.g. operational, safety, security, financial, reputational, regulatory, strategic, investment, infrastructure, people, technology, knowledge etc. (See appendix A1 - page 104 for more details)

- **Risk Criteria**

  Terms of reference (criteria) against which the significance of identified risk (to an organisation) is evaluated. Risk criteria are typically based on (internal and external) organisational objectives

- **Risk Evaluation**

  Process of comparing ***Risk Analysis*** results with ***Risk Criteria*** - to determine whether or not a specific risk under consideration is acceptable (tolerable) or not to the organisation concerned. Risk evaluation also assists with decisions to be made by the organisation with regards to use (if any) of risk treatments / controls

- **Risk Identification**

  Process of finding / recognising and describing / documenting risks (via / together with associated threats and vulnerabilities where appropriate) to the organisation

- **Risk Management**

  One definition:

  A process used to:

  - Identify actual and / or potential ***threats*** to an organisation's key product / services / operations + their associated (subordinate) key main + (in turn) key supporting activities + all associated processes *(**Threat** Identification)*
  - Estimate the ***likelihood*** (probability, frequency, chance etc.) & potential ***degree*** (effects, consequences etc.) of the (typically) adverse ***impacts*** of such threats on the organisation's key product / services / operations + their associated (subordinate) key main + (in turn) key supporting activities + all associated processes *(Risk **Analysis**)*
  - ***Evaluate and Prioritise*** the results of the ***risk analysis*** according to an agreed formula *(Risk **Assessment**)*
  - Provide information to enable an associated ***risk management control programme*** / ***action plan*** to be implemented *(i.e. an appropriate **Risk Strategy** + associated (Tactical) **Risk Treatments** / Solutions / Controls etc.)*

  Note - '***Enterprise Risk Management*** (ERM) typically differs from 'conventional' risk management only in terms of scope e.g. 'operational' type aviation activities are subject (mandatory) to the ***Safety Risk*** management process as per ICAO's Safety Management System (SMS) requirements

  Should the organisation concerned decide to additionally 'roll out' risk management to the **entire** organisation (i.e. not just those departments / business units related ***directly*** to aviation [flight] operations) - then this might reasonably be termed ERM. See appendix A2 - page 107 for more details

..... *& another definition*

Risk Management is an overall process - comprising sequentially:

Threat Identification - identifies and describes the '***threats***' (and the associated '***vulnerabilities***' [whereby a threat might be 'facilitated' to actually occur]) which could affect the successful achievement of an organisation's business objectives

Note - this might involve use of historical data, theoretical analysis, informed and expert opinion, consideration of stakeholder's / other interested parties' needs etc.

Threat (Risk) Analysis - used to understand the nature of ***identified*** threats - and to estimate (should such threat be realised [i.e. actually occur]) the potential (typically [but not always] adverse) **impact** level of same - ***combined*** with the estimated ***probability*** of occurrence

Note 1 - Threat / risk analysis provides the basis for the ***next*** step i.e. risk assessment / evaluation & associated decisions required (regarding choice of associated risk treatment(s) / solutions / controls required to avoid and / or mitigate the consequences of a realised threat)

Note 2 - Threat / risk analysis typically involves some form of personal 'estimation' - which is necessarily 'subjective' by nature - to a greater or lesser degree

Risk Assessment / Evaluation - used to compare identified risks with the organisation's ***defined risk criteria*** / ***risk appetite*** (latter typically documented in a 'Risks Register') in order to determine whether or not a specified level of risk is acceptable / tolerable.....and to assist in the potential selection of risk treatments (solutions / controls) which might be deployed, to manage each identified risk - as required

Risk Strategy + associated ***Risk*** Treatments (Solutions / Controls etc.) - any risk assessment results considered '**unacceptable** / **not tolerable**' will require application of an appropriate risk strategy + associated (tactical) risk treatments (solutions / controls) etc. - to the extent that (in one way or another) the risk becomes acceptable. Where the latter is not possible the risk will need to be removed - which will probably have the knock-on effect of cessation or modification of the associated activity / process etc.

..... *& one more definition*

Risk Management (RM)

The culture, (supported by associated processes, structures and resources) put in place by an organisation, to effectively manage potential opportunities and risks, based on the declared and current '***risk appetite***' of said organisation

As it is not possible (or desirable) to eliminate **all** risk, the objective is to implement cost effective processes which reduce risk to an acceptable level

AND / OR to reject unacceptable risks

AND / OR to treat risk via financial interventions i.e. transfer the risks to insurance organisations or similar

AND / OR treat risk by organisational interventions, one of which may be accomplished by the use of ***appropriate BC strategies*** *(in the form of BC tactical solutions / treatments / controls etc.)*

- **Risk Register**

  A comprehensive, documented list of ***organisational*** risks by category (graded / prioritised according with regards to probability of occurrence and potential [typically {but not always} adverse] impacts) - to which appropriate risk treatments / controls / solutions etc. ***might*** be assigned

  An example of a real risk register (for a specific country in this case) can be found by following the below link:

  https://naru.org.uk/wp-content/uploads/2017/10/UK-National-Risk-Register-2017.pdf

- **Risk Tolerance**

  Risk tolerance is the practical application of 'risk appetite' to an organisation's ***specific objectives***

  Whilst risk appetite relates to a broad, strategic ***concept*** - risk tolerance applies (at the tactical / operational [hands-on] level) to the task of actually achieving what needs to be done (if anything) within that concept

- **Risk Treatments** (Risk Solutions / Controls)

  There are typically five ***treatments*** which determine how ***threats*** to an organisation's key product / services / operations / key activities etc. can be ***'risk managed'*** (modified) in order to eliminate or reduce the associated probabilities of such threats occurring and / or if they do occur, mitigating the associated impact(s)

  1. **Avoidance** - exiting (or not even starting) activities giving rise to unacceptable risk
  2. **Reduction** 1A - taking action to prevent / reduce the **likelihood** (**probability**) of risk occurrence

3. **Reduction** 1B - taking action to ***reduce*** / ***mitigate*** the *consequences* of 'realised' risks i.e. plan to manage / 'treat' the ***impact***(s) of risk after it has actually occurred. One (but only one of several) methods of achieving this is by use of appropriate ***Business Continuity*** measures

4. **Transfer** and / or **share** (all or a portion of) the risk e.g. via insurance; partners; suppliers etc.

5. **Accept** - i.e. take no action e.g. due to 'acceptability' of the particular risk; due to result of a cost / benefit analysis; in line with an organisation's declared risk appetite etc.

For the purposes of *this* guideline document only - sub-paragraph 3 just above relates to the use of ***business continuity measures*** (solutions / treatments / controls etc.)

Re the latter, choice of which to use, when, how, in what circumstances and by whom - are collectively decided by formulation of overarching, associated BC '**Strategies**' (latter title changed in late 2019 to 'BC Strategies and Solutions' - such solutions relating tactically to 'what needs to happens next' i.e. after the strategies have been formulated and approved

'What happens next' refers to the formulation and application of the actual business continuity measures etc. required)

Typically, specific 'objective based' ***risk tolerances*** permit the appropriate department (and / or business unit and / or individual) a degree of 'flexible (tactical / operational) risk taking variance' in achieving the specific objective, whilst remaining within the organisation's declared, current & overall (strategic) ***risk appetite***

Nevertheless, such risk tolerance measures still require pre-approval, documentation, communication and regular monitoring / review

- **Significant**

A generic term (defined here for the purposes of this guideline document only) - meant to convey that 'whatever' it is that is considered ***significant*** (typically being the potential and / or actual consequences [impacts] of disruption on an organisation's activities, processes, resources etc.) is serious enough to require analysis and assessment from the Risk Management and / or Business Continuity viewpoints - and 'acted upon (treated / controlled)' in some appropriate way - if the circumstances so require and permit

- **Single Point of Failure** - (SPOF)

An activity which depends on a single resource (including a person where appropriate) - which is **not** replaceable should it become unavailable for whatever reason. Such unavailability invariably causes disruption of the associated activity / process etc.

- **Societal Security** (Since 2015 known as '***Security and Resilience***')

  An umbrella title used by the International Organisation for Standards (ISO) to cover a number of generic / related 'disciplines' - covering a particular genre of its standards and supporting documents - which it (ISO) produces / sells e.g. Risk Management; Business Continuity are included

- **Stakeholders** (See: 'Other Interested Parties')

- **Stakeholder** (Other Interested Parties) **Analysis**

  A 'business tool' which can be a useful starting point in the essential '***understanding the organisation***' task - the latter being an essential requirement when introducing and implementing BCMS into an organisation

  This analysis quite simply requires a brainstorming session(s) (by the organisation concerned) to identify all possible stakeholders / other interested parties associated in some way with said organisation's 'continuity of operation'

  The results are then placed in an initial order of importance (related to what they [stakeholders etc.] ***expect*** from the organisation and vice versa - such expectations being listed alongside the associated stakeholder / interested party concerned)

  This initial list is then used to assess the adverse impact of a disruption on such expectations and, if necessary, the order of importance of the initial list revised

  Finally (and the main reason for this analysis) the information acquired is used to ***ASSIST*** in **identifying** and **prioritising** ('scoring' by degree of urgency with regard to continuity of operation) the organisations **key products / services / operations** etc. (together with associated key main and key supporting activities [+ associated processes] + their inter-relationships, inter-dependencies, resource requirements etc.)

- **Supply Chain**

  A series of linked processes beginning with the acquisition of raw material - and ending with the delivery of product / services / operations to an end user (customer). The supply chain may include vendors / retailers, manufacturers, logistic services providers, distributors and distribution centres (internal and external), wholesalers etc.

- **Threat** / Hazard

  One definition:

  Something significantly undesirable etc. - which potentially ***might*** happen (to something, someone)

  ..... *& another definition*

  Potential cause of an undesired / unwanted incident which might result in harm to persons, assets, organisations, the 'community', the 'environment' etc

  Note- the words 'threat' and 'hazard' can be used interchangeably in CRPM Part 3 - Volumes 1 and 2. However, the interested reader should note that 'hazard' has a related but significantly different interpretation when used in the aviation related ICAO 'Safety Management System - SMS' (particularly 'safety risk management') context

- **Top Manager / Top Management** (TM)

  An organisation's most senior manager / top management team (e.g. Board of Directors) who / which directs and controls an organisation at the highest level possible. Amongst many other accountabilities TM has the power to delegate authority & provide resources within the organisation

  Where the scope of a BCMS does ***not*** includes the entire organisation - then the 'top manager' will typically be the most senior person in overall charge of each of the organisation's departments / business units which ***are*** subject to (within the scope of) the BCMS

- **Understanding the Organisation**

  A traditional (but possibly confusing) and fundamental business continuity term / concept which, in 'plain speak', refers to the following 'building block' activities, which need to be accomplished during the early stages of the '**DO**' element of the '**P**LAN, **D**O, **C**HECK, ACT' cycle - when introducing a BCMS into an organisation:

  - Stakeholder (Other Interested Parties) Analysis
  - Business Impact Analysis (BIA)
  - Risk Assessment (RA)
  - Business Continuity Requirements - Resources Analysis

  When the above has been completed, analysed and approved - the results are used to formulate '**BC Strategy + BC Tactical Treatments** / Solutions / Controls' etc. - and 'everything else' (business continuity [BCMS] wise) follows on from there!

- **Verification**

  Confirmation (via use of objective evidence) that specified requirements have been met

- **Vulnerability**

  One definition:

  A potential means of exposure to realisation of a threat(s). For example, fire is a ***threat*** to a particular facility

  Associated ***vulnerabilities*** which might enable this threat to be realised (to actually happen) include no alarm system; no fire extinguishers; no other fire suppressant system(s) (e.g. sprinklers); no associated training and exercising for 'interested parties' (e.g. 'staff' working at that facility) etc.

  ..... *& another definition*

  Process of identifying and quantifying 'something' which (the latter) creates a susceptibility to realisation (actual occurrence) of an associated threat / hazard which, if so realised, might have (typically) undesirable consequences (e.g. for an associated organisation; individual; service; product etc.)

  Risk Management (of which 'Business Continuity' is just one of several components) techniques are typically used to 'control / manage / mitigate etc.' threats and their associated vulnerabilities

  ..... *& another definition*

  Intrinsic properties of 'something' creating susceptibility to an associated risk source which, if realised, might lead to an 'event' (incident etc.) with a (typically undesirable) consequence(s)

Deliberately Blank

Finally - (before looking at the appendices & possibly moving on to CRPM Part 3 / Volume 2

On this and the next page is a brilliantly simple example of what Business Continuity (+ Risk Management etc.) is all about:

Firstly, take a look at (activate) the below Youtube video clip:

https://www.youtube.com/watch?v=DDS833zadfI

Secondly (assuming that you have now viewed the video and based on what you might have picked up already by reading ***this*** CRPM Part 3 / Volume 1 guideline document up to this point in time???) - think up / write down how (assuming that you are the 'boss' of the 'workers / staff' seen in the above clip) very brief (say a sentence or two for each item listed just below) notes for how you might:

a. Recognise (work out) in advance that such a situation might occur

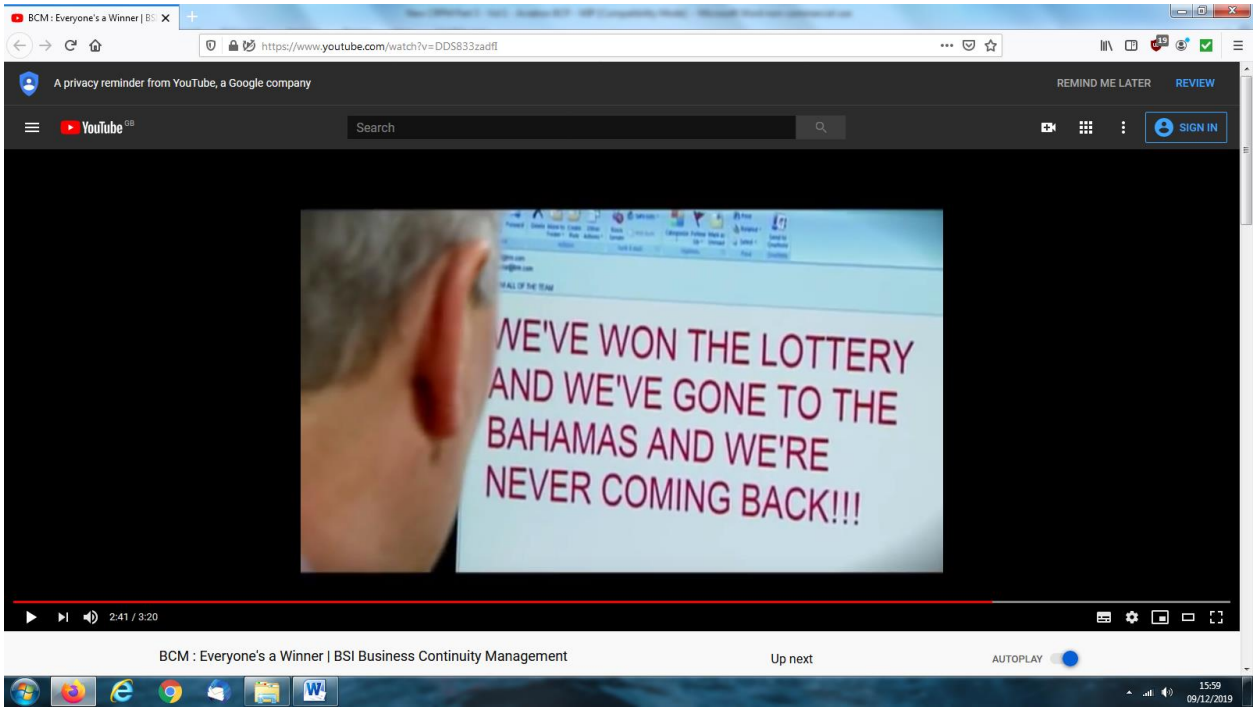
b. Prevent or account for such a situation happening in the first place

c. If you are having trouble finding an answer to b. above (which works; is feasible / reasonable; is not too expensive; is ethical / lawful etc.) then see d. below. Even if you are not having trouble, still see d. below

d. Assuming that the situation 'has now happened' - what you will do to (try to) mitigate the immediate adverse consequences (to you and your business) and how (if) you will be able to recover (in the future) your business operation to its original (fully working) status?

   Assume that your business *did* make profits for the preceding 3 business years but that they (profits) were not 'making you rich'. Also assume that you had insurance - but that it did not cover the situation (risk) described above

Lastly - see next page for how to best manage (from Risk Management / Business Continuity viewpoints) the above scenario



THREAT = Entire Workforce jointly 'Wins the Euromillions Lottery'

VULNERABILITIES = None

RISK = Permanent and Concurrent Loss of (Current) Entire Workforce

POTENTIAL IMPACT = Catastrophic

LIKELIHOOD = Never Happen

STRATEGY / SOLUTION = Do Nothing

WHY DO NOTHING? = * Odds against winning = 140, 000, 000 to 1 for each ticket purchased i.e. so incredibly low that the ***risk can be accepted*** by the employer

* If you were to buy 1,000 lottery tickets per day, it would statistically take almost 400 years before you have a win

Deliberately Blank

APPENDIX A1

RISK CATEGORIES - MORE INFO

There is typically no consensus on how an organisation might generically ***categorise*** the types of risk which could impact upon it. One method 'links together' risk as follows:

- **Hazard Risk** arises e.g. from property / facilities, (legal) liability, personal loss exposures etc. - and is generally mitigated (treated to reduce impacts) by taking out appropriate insurance
- **Operational Risk** typically relates to 'failure' in a people associated context and also in business associated processes, systems (including ICT in particular), controls etc. One of several methods used to mitigate operational risk uses **Business Continuity** measures (controls / treatments / solutions etc.)
- **Financial Risk** - arising from the effects of market forces, crime etc. on financial assets and / or liabilities. This risk is typically sub-divided further into:
    - Market Risk
    - Credit Risk
    - Liquidity Risk.....and
    - Price Risk
- **Strategic Risk** - e.g. due changing trends in the economy and society, changes in the political and competitive environments, demographic shifts etc.

Hazard and **Operational** risks might be classified as '***pure***' risk - whereas **Financial and Strategic Risk** might be regarded as '***speculative***' risk

Organisations typically categorise risk in line with what it is that the particular organisation 'does' - so the information provided above must be regarded as typical only e.g. some will regard 'legal risk' as slotting into the 'operational' risk category instead of the 'hazard' risk category

Moreover, such information must not be regarded as being exhaustive i.e. there are typically more risks over and above those listed

For 'visual impact' purposes, such categories might be envisaged as lying in 'quadrants' of a circle - as per the diagram on page 106. This then lends itself to better interpretation as related to 'real life'

For example, take a new (start-up) business organisation (***Company X***) which manufactures mechanical parts (and is based) in ***Country A***, using a largely automated production line. It sources its raw materials from ***Countries B*** and **C** and sells the finished product in ***Country D***

- In the Hazard Risk quadrant, Company **X** should include 'property' related risks for its facilities, plant, equipment etc. - such risks possibly being associated e.g. with fire, natural disaster, utilities (power / electricity) failure - and so on

  It should also include risks associated with injury to employees; risk of liability associated with use / quality / safety of its product etc.

- ***Operational*** ***Risk*** could arise from e.g. employee turnover, the inability to find skilled staff etc. There would also be 'business process' risk related e.g. to how the business manages its supply chain; ICT risks to the automated manufacturing process etc.

  Another way of expressing 'operational risk' might be:

  '.....The risk of loss resulting from inadequate or failed internal processes, people and systems - or from external events - but might be more simply viewed as the risks arising (in general) from just carrying out an organisation's normal business functions

  Operational risk exists in every organisation, regardless of size and / or complexity.....'

  It is worth repeating here that:

  One of several methods used to control / treat operational risk is by use of Business Continuity measures

- Financial Risk might arise for a number of reasons - e.g. price (currency) exchange rate risk for country **A** with regard to countries **B**, **C** and **D**; price risk for procuring raw materials and other essential supplies etc.

  If the country **D** customer is slow to pay its bills, liquidity (cash-flow) risk could materialise for Company **X**

- Strategic Risk includes competition; economic factors affecting consumer demand; political and security etc. risks in countries **A**, **B**, **C** and **D** - and so on

A slightly different method adds two further risk categories i.e. '***Compliance*** Risk' and '***Reputational*** Risk'. However, for the purposes of this document (the one you are now reading) we include both here as part of Operational Risk

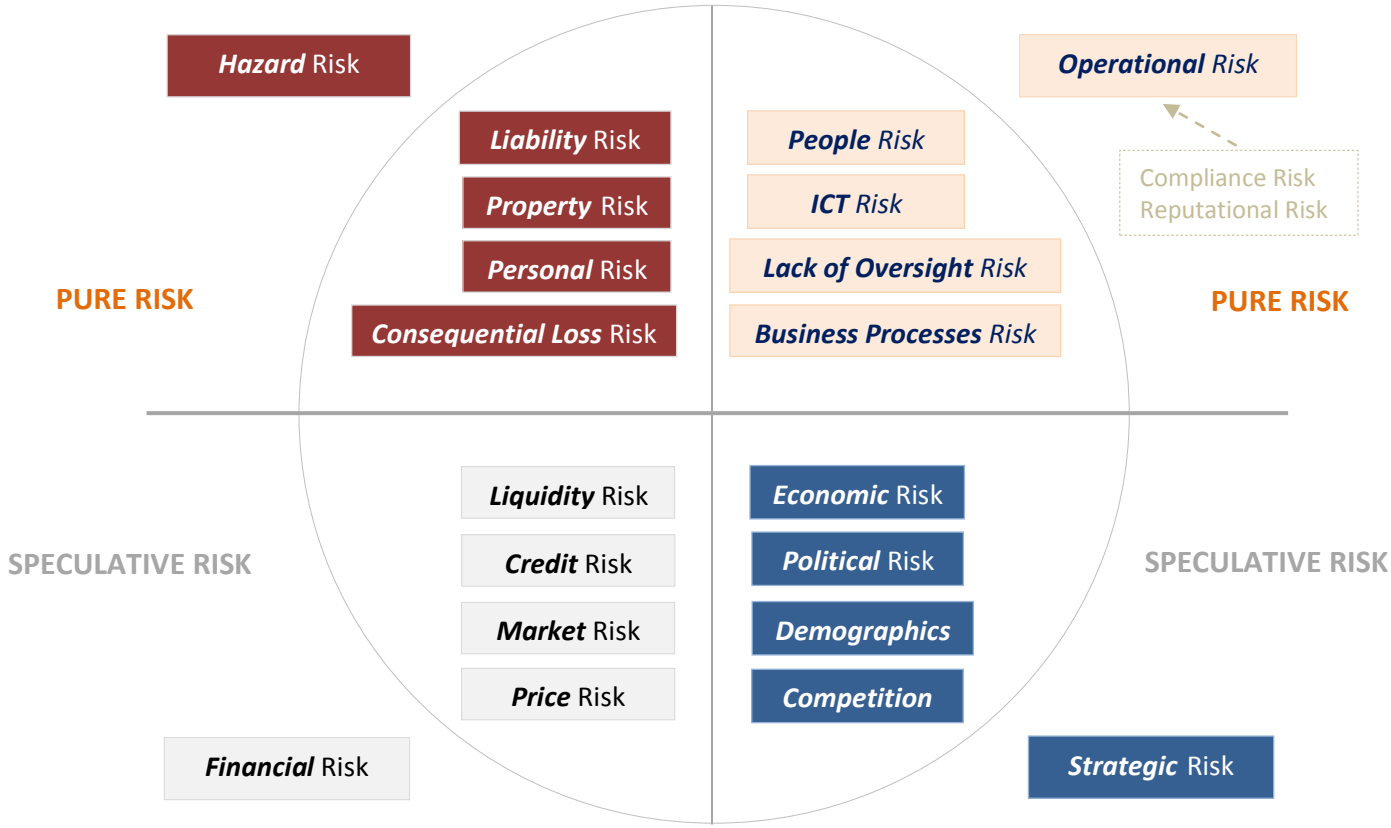


Diagram: Typical Risk Categories (List is not exhaustive)

For more useful information on 'risk', follow the links shown below in order 'top to bottom'

https://business.tutsplus.com/tutorials/the-main-types-of-business-risk--cms-22693

https://business.tutsplus.com/tutorials/how-to-measure-risk-in-your-business--cms-22763

https://business.tutsplus.com/tutorials/effective-risk-management-strategies--cms-22887

https://business.tutsplus.com/tutorials/how-to-protect-your-business-with-the-right-insurance--cms-22963

APPENDIX A2

Enterprise Risk Management

Definition 1:

'Enterprise Risk Management' (ERM) is the process of ***coordinated*** risk management, which places emphasis on ***co-operation*** to ***direct*** and ***control / manage*** an ***ENTIRE*** organisation's ***FULL*** range of risks. ERM thus offers a '**holistic**' framework for effectively managing uncertainty, responding to risk and harnessing opportunities (risk appetite) as they arise

Unlike previous risk management practices (which often tended to be run as separate, un-coordinated 'silos' [within an organisation]), the concept of ERM embodies the notion that risk management cuts across an entire organisation

ERM's goal is to better understand the organisation's resistance to ***ALL*** of its key risks and thus better manage risk exposure to the level desired (including 'risk appetite') by top management

Definition 2:

ERM is the process of planning, organising, leading and controlling an organisation's activities - in order to minimise the effects of risk on its capital and earnings. ERM includes financial, strategic and ***operational*** risks + those associated with accidental losses

More recently, external factors have fuelled a heightened interest by organisations in ERM e.g. industry and government regulatory bodies, as well as investors, have begun to scrutinise companies' risk-management policies and procedures. Furthermore, boards of directors are increasingly being required to formally review and report on the adequacy of risk-management processes in the organisations they administer

'**Operational Risk**' is the prospect of loss resulting from inadequate or failed procedures, systems or policies. It includes:

- Employee errors
- Systems failures
- Fraud and other criminal activity
- Any event which disrupts ***business continuity***

Most organisations accept that their people, processes etc. will (at one time or another and for whatever reason[s]) be subject to 'problems' and thus contribute to ineffective operations. In evaluating operational risk, practical remedial steps should be emphasised in order to identify and eliminate (or at least mitigate) such problems in a timely manner

Poor operational risk management can hurt an organisation's reputation, cause financial damage, impact adversely on the 'workforce' etc. How much of the latter an organisation accepts, combined with the cost of correcting same, determines its 'risk appetite'

Deliberately Blank

Appendix B

Horizon Scanning

DEFINITION

(As related to the Risk Management / Business Continuity / Contingency Planning Context)

The systematic examination of potential threats, opportunities and likely future developments - including (but not restricted to) those at the margins of 'current' thinking and planning

Horizon Scanning may explore novel / unexpected issues (sometimes referred to as * '***Black Swan***' events) in addition to the more familiar problems and threats

* For more details re the various types of 'swan' ('black', 'grey' and 'white') events - see separate document CRPM Part 3 / Volume 2 - 'Case Study 7'

Background

An 'annual' horizon scan of appropriate, actual and potential business / organisational risks and threats is compiled (on a ***worldwide*** basis) by the UK's * 'Business Continuity Institute' (BCI) in conjunction with the UK's 'British Standards Institute' (BSI). 2017 was, for example, the 6th such scan in successive years

* Although the BCI and BSI are UK organisations, they have thousands of members all over the world - and input from same is used to compile the annual horizon scans - as is evidenced from the following extracts from the 2016 and 2017 Horizon Scans respectively:

'……*In association with BSI, the annual BCI Horizon Scan Report seeks to identify near-term threats to organizations worldwide. It also measures the sentiment of business continuity (BC) and resilience professionals by indicating their level of concern to different risks and threats*

As a respected industry resource, the report complements in-house analysis and benchmarks horizon scanning activity among organisations across regions and industry sectors. Data cited in this report was obtained from a survey which began in October 2015 and ran for eight weeks. ***568*** *organizations from* ***74*** *countries participated in this study……*'

'……*In association with BSI, the BCI Horizon Scan Report is based on an annual study which tracks near-term threats to organizations across industry sectors globally. In its sixth edition, this study measures concern over specific threats as reported by business continuity and resilience professionals. The report also captures disruption caused by these threats, offering a basis of comparison between the level of concern and actual incidents*

Over the years, this report has become a highly anticipated industry resource as it complements in-house analysis and assists horizon scanning activity. The report features results of a survey distributed from October 2016 and ran for four weeks; ***726*** *organizations from* ***79*** *countries participated in this study……*'

The general objectives of the horizon scan are to:

- Check and confirm previous and current types of risk (i.e. are they still relevant / accountable?) and to……
- Try to identify and quantify new (potential / future) types of risk materialising, which could eventually test (adversely impact upon) societies, organisations etc. worldwide - to a greater or lesser degree

By its very nature the 'forward-looking' aspect of horizon scanning is imprecise (in a similar way to the imprecision of longer range weather forecasting!). However, it is significantly better than nothing and, as it is updated annually, can be used by risk management, business continuity and emergency / incident planners to tentatively update their risk registers and contingency plans - where thought appropriate

It is strongly recommended that all involved closely with risk management, business continuity and emergency / crisis etc. response planning - acquire and take due note of said horizon scans. They would also be well advised to conduct and act on their own 'bespoke' horizon scans - where the circumstances of their own societies, organisations etc. so require

To find a particular BCI / BSI horizon scan(s) via an internet search - use something like the following words. (The *'year'* to insert should be the one that you are interested in of course):

'.....BCI / BSI horizon scan *2020*.....'

- For the interested reader the 2019 BCI / BSI horizon scan is linked to **HERE**
- Similarly, the 2020 version can be found **HERE**

Note of Interest / Context

Re the 2019 BSI Horizon Scan (published around March 2019), 'Pandemic' (Disease Outbreak) featured on a table of the top 19 areas of 'risk and threat assessment' concern for the previous 12 months. It was positioned 19th (out of 19). The 2020 version (published around March 2020) had 'promoted' pandemic to position 15 (again, near the bottom of the 19 listed) in its section which looked ahead for the next 12 months

We now know that the COVID-19 pandemic made its first overt appearance in Wuhan, China around December 2019. As at mid-June 2020 around 7.5 million infections had been reported (in reality there were ***many*** more infections than this that went unreported, for various reasons) and getting on for half a million deaths (again, in reality, ***many*** more deaths than this went unreported, for various reasons)

With the 21st century already having seen previous outbreaks of SARS, Swine-flu, MERS and Ebola, and given the potentially catastrophic events of predicted 'bird-flu' pandemics (re mutations of the H5N1 and H79N virus strains so as to be contagious human to human) which had been forecast since around 2002 - hindsight might have merited higher placings for 'disease outbreak' than those referred to in the 2019 and 2020 horizon scans above

One adverse consequence (amongst many) of COVID-19, which ***SHOULD*** have been predicted and acted upon as a top priority (but was not by most countries), was the inadequate pre-procurement and stockpiling of appropriate Personal Protective Equipment (PPE) for use by medical / health staff and other appropriate responders. This omission possibly cost thousands of lives

FOOTNOTE

From: 'Continuity Central.com' (below message released in ***March 2020***)

'BCI Publishes its Annual Horizon Scan Report'

'..... BCI has released the 2020 version of its Horizon Scan Report (see link [this page further above]). Sponsored by BSI, the report reflects the concerns of business continuity and resilience professionals when looking ahead to anticipated threats

Interestingly, whilst COVID-19 is currently front-of-mind for business continuity managers around the world right now, ***when the Horizon Scan SURVEY was conducted*** (probably sometime in the second half or 2019?) the threat category ***'Non-occupational disease'*** was ranked as ***second from last*** in the list of ***Future Threats*** (see page 20 of that report). If the survey was conducted currently, this result might (would) be very different .....'

Deliberately Blank

Appendix C

Business Continuity Planning / **Business Impact Analysis** (BIA)

IMPACT CATEGORIES

An early task in preparing a BIA is to plan for and produce an associated ***questionnaire***

An important part of the latter is targeted at identifying / choosing the various '***impact*** *(or 'consequence')* ***categories***' of most relevance (e.g. as related to mission / objectives / strategy / operations / business / location etc.) to the organisation. ***This is important*** and is worth spending time and effort to get right

Question: What is the meaning of '***impact*** (consequence) ***category***' as used in a risk management / business continuity context - more particularly that related to Risk Analysis (RA) and associated Business Impact Analysis (BIA) type activities?

Answer: Firstly, see again list (in this document) on page 5

Almost everything listed there (threats and risks) can be similarly applied - but now as / in a 'functional' role related to associated, potential impact (consequence) categories

Very simplistically and in summary, most organisations will probably need to consider ***at least*** some of the following subject matter areas when dealing with 'impact categories:

* Financial
* Operational
* Brand, Image, Reputation, Crisis Communications
* Death / Injury / Health
* Interruption of Services (for whatever reason e.g. Supply Chain)
* Performance
* Stakeholder / other Interested Parties
* Statutory / Legal / Regulatory / Best Practice / Contractual
* Essential Infrastructure; Services; Equipment; Buildings etc.
* Loss of Workforce
* War / Conflict
* Crime (all types)
* Customer Service
* Environmental (People & Natural [including weather])
* Disaster (Natural / Manmade)
* Safety and Security

Final choice of which impact categories should be actually accounted for are those which best relate to the core mission / strategy / operations / business / location etc. of the particular organisation concerned

Additional categories (over and above those listed above), if any, might be derived from what is uniquely important to the particular organisation with regards to 'what it does' - which, if disrupted for an * 'appropriate' period of time, would lead to the more / most serious, negative consequences

* An 'appropriate period of time' might range from a few seconds (immediate, remedial action required) to hours, days and sometimes considerably longer e.g. months and even years

Note that there is no ***universal*** list of impact categories which ***applies*** to ***all*** organisations

Note: The BIA questionnaire (referred to on the previous page) is typically targeted at those in the organisation (typically employees and equivalents in the most appropriate jobs and at the most appropriate levels / grades [rarely at a senior level / grade]) considered to best have a valid input as to the organisation's operations/ processes / services etc. which, if disrupted for an appropriate period of time, would have the most adverse impacts e.g. on:

- The organisation itself
- On its customers (as appropriate and in the wider sense of the term e.g. we might be referring here to 'patients' [and their families also] if the organisation was a 'hospital')
- On its employees
- On the environment
- On the 'surrounding community
- On the organisation's shareholders and other 'interested parties' etc.

It is strongly recommended that the person conducting the BIA uses the questionnaire as an 'aide memoire' when ***personally interviewing*** those providing the responses (i.e. completing each questionnaire him / herself using the responses / results from the ***face to face interviews***)

Second best choice might be to distribute the questionnaires to those chosen to complete them; brief the latter (probably together as a group) on what is required and how to go about it - and designate a reasonable time period for completion and return of said questionnaires

During this latter period the person conducting the BIA should be reasonably available to answer questions; provide advice etc.

For the purposes of this Annex C, questions (in the questionnaire) related to '***impact categories***' should be carefully thought out with the aim of getting the most useful and relevant responses

As to getting across the desired meaning / understanding of what is meant by 'impact category' - this should be accomplished during the face to face interviews and / or at the group briefings already mentioned above

A Simplified Method of Identifying Impact Categories for use with the BIA

1. Split up the potential categories into quantitative (money etc.) impacts and qualitative (non-money) impacts - as appropriate. This provides for a rounded / balanced / clearer view of the 'damage' that might be caused by disruptions of various lengths

2. Limit the number of categories to the absolute minimum necessary to achieve what is required. Too many categories can make the BIA related * interviews go on too long and possibly also confuse and / or bore the participants

   * See again the 'note' on the previous page - if so required

3. Ensure that the categories are consistent across the whole of the organisation (or the part of the organisation subject to the BIA - as appropriate) etc. This allows you to measure 'like for like' when gauging the impacts of potential disruptions

4. Choose categories best reflecting the core mission etc. of the organisation's business

   For example:

   - Hospitals might include 'patient care and safety'- as a typical 'qualitative' impact category
   - Universities might similarly include 'student experience and safety'
   - Manufacturing firms might typically have a qualitative category related to 'supply chain' operations
   - Banks might use 'penalties, fines, sanctions etc.' (e.g. i.e. as imposed on the bank itself - typically for some form of 'transgression' against banking 'norm's) as a quantitative category etc.
   - Almost all organisations will need to include (to a greater or lesser degree) 'brand, image and reputation' type considerations
   - ..... and so on

   To reiterate, it is important thing to think carefully about the core mission of your organisation etc. then research and select the most appropriate impact categories

5. Once you have tentatively chosen the impact categories, circulate them to appropriate departments, business units etc. (within the organisation) for review and feedback. Obviously, the ideal is to have unanimous agreement on the final categories chosen

The Most Common Mistakes Made in Identifying Impact Areas

- Having too many BIA impact categories
- Mistaking quantitative impact categories for qualitative ones and vice versa
- Choosing the wrong categories for the type of organisation concerned

Examples from Four Major Industries

The table (next page) shows a ***limited number*** of examples of the impact categories commonly chosen in four major industries: finance, healthcare / hospitals, insurance and aviation

The impact categories shown are reasonable 'example' choices for these types of organisations

In reality more impact categories would almost certainly be chosen than those shown for each type of industry in the table

However (and as already mentioned further above) too many categories might not a good idea. It is suggested that ***up to*** about 8 impact categories (if this is a possibility for the organisation concerned e.g. smaller / simpler organisations may actually only have a smaller number of impact categories to consider in reality e.g. 2 or 3) maximum be chosen, if so needed

It will be a very rare organisation indeed which might genuinely have the need to choose more than 8 impact categories:

INDUSTRY (Organisation)	**QUANTITATIVE** Impacts	**QUALITATIVE** Impacts
Finance	Loss of Revenue	Customer Service
	Increased Operating Expenses	Legal / Regulatory Requirements
	Penalties, Fines & Sanctions	Brand, Image & Reputation

INDUSTRY (Organisation)	***QUANTITATIVE*** Impacts	**QUALITATIVE** Impacts
Healthcare *(Hospital)*	Longer Waiting Lists	Patient Care and Treatment
	Not enough Doctors, Nurses etc.	Patient Safety and Security
	Inadequate Medicine / Drug etc. Resources	Staff adequately qualified & experienced

INDUSTRY (Organisation)	***QUANTITATIVE*** Impacts	**QUALITATIVE** Impacts
Insurance	Inadequate Customer Base	Customer Service
	Competition	Legal / Regulatory Requirements
	Profit Margins too Small	Brand, Image & Reputation

INDUSTRY (Organisation)	***QUANTITATIVE*** Impacts	**QUALITATIVE** Impacts
Passenger Airline	Prices / Fares	Customer Service
	On-time Performance	Legal / Regulatory Requirements
	Numbers of Passengers & Amount of Freight	Brand, Image & Reputation
	Route Network	Modern Aircraft Fleet

'Weighting' the Chosen Impact Categories

When the most appropriate impact categories for the organisation concerned have been identified, it is then necessary to determine the 'weighting' to be used for each

Weighting is the process of ***ranking*** the impact categories ***in order of 'how important it is*** to the organisation that disruption to each category be ***avoided*** / ***minimised*** etc.'

Typically (but not always) the more important it is to avoid etc. disruption to a particular category, the quicker such disruption needs to be addressed, if it ever actually occurs

Note that 'weighting' is ***not*** a ranking of ***services, product etc.*** in terms of how important they are to the organisation. Rather, it refers to the ***degree*** of 'avoidance/ minimisation' measures required - as referred to above

One (but only one of several) way of expressing 'weighting' is to assign a percentage value to each impact category of concern, with the sum totalling 100 percent. For convenience and clarity / simplicity only, this is the weighting method described here

This percentage value is the estimate of the negative impact (on your organisation's key mission, operations etc.) of having that function interrupted e.g. the possibility of an electricity failure in a hospital (and particularly its operating theatres) would score (be weighted) very highly

Why It's Important to Weight BIA Impact Categories

Where more than one type of significant disruption impacts concurrently on an organisation, it will typically be necessary to decide which requires most resources to be deployed most quickly in order to restore operations (i.e. prioritise restoration of the interrupted functions in order of which could cause the most 'damage' to the organisation / business etc.)

If e.g. two of the organisation's main processes etc. are disrupted concurrently, it should be relatively easy to assign recovery priorities (weightings). But what if there are e.g. 8 areas so impacted?

It will be too late (on the day) to think about which needs to be addressed in what priority order, with what resources (including people) etc. Therefore, it is necessary to restore first the functions whose interruption is causing the most 'damage' (having the greatest adverse impact[s] - whatever they might be)

Another reason for weighting impact categories relates to 'human nature' - i.e. the tendency we have to rate what ***we*** (ourselves) do as being more important than what others are doing

For example, when an organisation's departments / business units are asked (during e.g. a BIA interview / questionnaire) how important their related inputs / outputs are to the organisation's mission / products / services etc. - many might consider them to be of critical importance. Not only is the latter unlikely in the majority of organisations - it would also be near impossible to deal with (if it were) re the 'weighting of impact categories' task

It is not unusual for a significant proportion (of an organisation's) personnel base to feel that what they 'do' is important - and in many cases they would be correct i.e. the organisation *would* be adversely impacted if they were not operational for any reason. But for some roles the adverse impacts might not be felt for days / weeks or even longer - whilst for others the consequences might be immediate (think hospital operating theatres again)

How to Weight BIA Impact Categories

The person(s) conducting the BIA should consult frequently with the 'management team' supporting the process. Gather the latter's inputs as to the identified impact categories + their respective rankings / weightings e.g. what areas do they think are the most important and in what proportion; then the next most important + proportion etc.

For example, a bank might basically prioritize its impact categories as follows:

1. Loss of Revenue
2. Decrease in Customer Service
3. Adverse impacts on Brand / Image / Reputation
4. Requirement to pay Penalties & Fines and / or to be bound by adverse Sanctions
5. Abide by Legal / Regulatory Requirements
6. Increased Operating Expenses

The bank now assigns a 'relative' percentage to each impact category based on its importance (to the bank). This is obviously not an 'exact science' but the top categories will typically make up the majority of the weighting percentage

Adding some fictional (but realistic) weighting percentages to the above list we might get:

- Loss of Revenue (25%)
- Customer Service (25%)
- Brand, Image and Reputation (20%)
- Penalties, Fines and Sanctions (15%)
- Legal / Regulatory Requirements (10%)
- Increase to Operating Expenses (5%)

The total of the weightings should add up to 100 percent of course

Based on the above weightings, the greatest adverse impacts of disruption (however it is caused and whatever might be its 'type') run (respectively) in scale from top to bottom and, consequently, this is the order in which they should typically be recovered and / or the underlying 'problem' area(s) addressed by the organisation

The Most Common Mistake

The most common mistake made in 'weighting' impact categories is probably not taking enough time, effort, consultation and research to make it as 'useful' to the organisation as possible (in what is, in reality, quite an 'unprecise by its nature' undertaking in the first place)

Remember - 'weightings' are essentially a human (and thus subjective) judgment call of what is e.g. most critical, less critical or not critical to an organisation's product / services etc. Nevertheless they are still used (as there is no viable alternative) to determine what is to be restored first, what next and what later etc. after a serious disruption type event or equivalent. The consequences of getting it wrong could be disastrous (in many different ways) to the organisation (and probably to others also)

Next

Following weighting of the identified BIA impact categories, the results are 'integrated' into the overall BIA process. For example, they are used to evaluate the quantitative (e.g. money / finance type matters etc.) and qualitative (e.g. operational effectiveness etc.) impacts of significant disruption to each impacted business process / equivalent function (under consideration) - over various periods of time

This in turn allows e.g. estimation of the associated ***Maximum Tolerable Periods of Disruption*** (MTPD) and associated ***Recovery Time Objectives*** (RTO) for the different business processes etc. under consideration in the BIA

* RTO and MTPD calculations are essential building blocks to the whole Business Continuity Plan of an organisation. Neither can be usefully derived without firstly undertaking a BIA - and a BIA will not deliver useful outputs without adequately identifying the appropriate impact categories (relating to the organisation of concern here) - and weighting them accordingly

* For brevity purposes MTPD and RTO are not explained further here as they are beyond the scope of this Appendix C

Conclusion

The most appropriate selection and weighting of (BIA related) impact categories is an important task which, if done well, will make a significant difference to the effectiveness of the BIA - and thus, in turn, the organisation' overall Business Continuity Plan

Note:

On the next page you will find a generic example of impact ***categories*** (otherwise known [with the same meaning] in this particular example as 'impact ***consequences***'

You will note that there are 8 categories listed horizontally across the top of the matrix. As this example is ***generic***, no particular business / organisation etc. is named / typecast (but it would be for real of course). The introductory text at the top of the matrix 'speaks for itself'

On the page after that you will find a different, generic example in more detail

And on the page after that is shown what might be considered to be a 'real life' example as might be used by a real, passenger ***airline***. It is provided in ***this*** CRPM Part 3 / Volume 1 document for interest and context purposes ***only***. It (and much more e.g. the Risk Assessment and Business Impact Analysis processes in full detail)) is described fully in (separate document) CRPM Part 3 / Volume 2

Business-Continiuty-Management-Business-Impact-Analysis-sample.pdf - Adobe Acrobat Reader DC

File Edit View Window Help

Home Tools Business-Continiut... Sign In

Risk/Business Impact Reference Table

The purpose of this table is to provide common language on how consequences (impacts) are evaluated and measured. This table illustrates various consequence categories that may be used in an agency's risk assessment process. A subset of these categories is used for business impact analysis. The categories should reflect the agency's economic, social and environmental responsibilities in relation to business continuity.

Level	Rank	Injuries	Financial loss	Interruption of service	Reputation and image	Operational efficiency	Performance	Stakeholder impact	Statutory
1	Insignificant	None	Less than $50,000 or .025% of operational budget	Less than 1 hour	Unsubstantiated, low impact, low profile or no news item	Little impact	Up to 5% variation in KPI or objectives	Inconvenience and delays to individuals	No noticeable regulatory/statutory impacts
2	Minor	First aid treatment required	$50,000 to $250,000 or .15% of operational budget	1 hour to 1 day	Substantiated, low impact, low news profile	Inconvenient delays	5% - 10% variation in KPI or objectives	Significant impacts on individuals but no noticeable impact on overall service delivery	Minor and temporary non-compliance with regulatory requirements
3	Moderate	Medical treatment required	$250,000 to $3m or 2% of operational budget	1 day to 1 week. Loss of building or workspace	Substantiated, public embarrassment, moderate impact, moderate news profile	Delays in major deliveries	10% - 25% variation in KPI or objectives	Major impacts on significant numbers on individuals, resulting in noticeable impact on overall service delivery	Short-term non-compliance with significant regulatory requirements
4	Major	Death or extensive injuries	$3m to $10m or 6% of operational budget	1 week to 1 month. Loss of building or workspace	Substantiated, public embarrassment, high impact, high news profile, third party actions	Non-achievement of major deliverables	20% - 50% variation in KPI or objectives	Major and long term impacts on individuals and overall delivery of services	Significant non-compliance with essential regulatory requirements
5	Catastrophic	Multiple deaths or severe permanent disablement	More than $10m or more than 6% of operational budget	More than 1 month. Loss of building or workspace	Substantiated, public embarrassment, very high impacts, high widespread news profile, third party actions	Non-achievement of major key corporate objectives	More than 50% variation in KPI or objectives	Permanent or debilitating impact on individuals and overall delivery of services	Long-term or indefinite non-compliance with essential regulatory requirements

19:59
23/03/2019

EXAMPLE ONLY

Also known as '***IMPACT** Category*'

Generic *BIA Reference Matrix* - used to formulate ***impact criteria*** (which in turn are used to provide ***impact assessment*** 'scores' for specified activities)

***CONSEQUENCE** Category* →	**Interruption**	**Op. Efficiency**	**Regulatory etc.**	**Financial**	**Reputational**	**Stakeholder**	**Injuries etc.**	**Other**
***IMPACT** Criteria* ↓	↓	↓	**IMPACT ASSESSMENTS**			↓	↓	
1. Negligible	< 2 hours	Minimal	Minimal	< .025% of op. budget	Minimal	Minimal	None	*TBA*
2. Moderate	2 - 12 hours	Slight reduction	Temporary (minor) non-compliances	.025 to .2% of op. budget	Low 'news' value	Some minor impacts	First Aid required	*TBA*
3. Significant	12 - 24 hours	Considerable reduction	Significant non-compliances in the shorter term	.2 to 2% of op. budget	Some damage - moderate news value	Significant impacts to some and / or minor impacts to all	Hospitalisation required	*TBA*
4.Serious / High / Major	24 hours to 1 week	Some key activities not deliverable	Significant to major non-compliances in the medium term	2 to 5% of operating budget	Major damage - high news value - stakeholders 'taking action'	Major impacts to some and / or significant impacts to all	Some critical injuries and / or deaths	*TBA*
5.CATASTROPHIC	> 1 week	Key products / services etc. not deliverable	Major non-compliances in the longer term / indefinitely	> 5% of operating budget	On-going viability of business threatened	Major and long term impacts to all	Mass critical injuries and / or deaths	*TBA*

The purpose of the above matrix is to provide a 'common language' on how impacts (on activities etc.) are evaluated and measured (the latter must be specific to what the organisation 'does' of course e.g. banking criteria will be different in some (but not all) areas to that used for airline operations). Note that this matrix is a ***generic*** example and is ***not*** targeted specifically at aviation related key activities etc.

EXAMPLE ONLY - AIRLINE OPERATIONS CONTROL CENTRE (OCC) - ***Comprehensive*** Version

BIA Template - Key Activities - ***Comprehensive*** ***Version of*** **Activity Impact Matrix** (Assuming airline operates 24H on a worldwide basis)

Activity & BIA Assigned Priority: Airline (ABCX Airways) ***OPERATIONS CONTROL CENTRE*** - OCC - **HIGHEST** Priority (e.g. 'Priority 1B')

Risk: ***Complete loss of OCC facility*** (e.g. due fire [the 'threat' in this example]. This '*risk*' would have been derived from a (separate) *RA*

Impact Categories ↓ / ***Impact Durations*** →	1-2 hours	3-6 hours	6-12 hours	12-24 hours	24-36 hours
Assess impact on ***passengers*** ops	2	2.5	3.5	4	4.25
Assess impact on ***cargo*** ops	2	2.5	3	3.5	4
Assess ***commercial*** impact	2	2	2.5	3	3.5
Assess ***financial*** impact	2	2	2.5	3.5	4
Assess ***reputational*** impact	1	2	2	2.5	3.5
Assess ***backlog*** (work catch-up) impact	2	2.5	3	4	4.25
Assess impact on ***OCC staff***	2	2.5	3	3.5	4
Assess impact on ***operating crew***	2	2	2.5	3	3
Assess ***legal*** / ***regulatory*** impact	2	2	2.5	3.5	4.25
Assess (anything else as appropriate)	*TBA*	*TBA*	*TBA*	*TBA*	*TBA*
Overall Impact Assessment of activity loss	***2***	***2.5***	***3***	***3.5***	***4***

Impact ***Categories*** by 'type'

Impact ***Assessments*** - graded ('scored') by degree ('weighting') of ***adverse*** impact criteria

Adverse Impact Criteria (Weightings): 1 = Minor; 2 = Acceptable; 3 = Significant; 4 = Major / Serious / High; 5 = Catastrophic

Estimated ***MTPD*** / ***MAO*** = **24 hours**

Calculated ***Initial RTO*** = **12 hours** *(Note may require 'adjustment' after accounting for 'knock-on' effects of associated interdependencies [if any?])*

MBCO = **50% recovery within 12 hours;** **75% within 18 hours;** **100% within 24 hours**

Maximum anticipated (adverse) impact assessment beyond about ***30 to 36 hours*** outage = **5**

Deliberately Blank

Appendix D

What has changed in ISO 22301:2019? (Compared to the 2012 version)

One Contribution:

ISO 22301:2019 is now in the final stages of release (expected at the end of October 2019)

The good news is that there are no earth-shaking changes in this version. Some of the important changes are:

- The Technical Committee 223 (Societal Security) is now merged into TC 292 (Security & Resilience). Mention of 'societal security' has been replaced in the objectives by 'security & resilience'
- The 2012 version was one of the first ISO standards to be produced in the 'High-Level Structure' format (now [2020] a common structure and core text for all ISO standards). Standards are becoming leaner, with crisp text and less prescriptive - and we can see the same here
- The introductory guidance section has been removed and placed in the forthcoming ISO 22313:2020 (latter is guidance document for implementing the requirements of ISO 22301 - it was published in February 2020)
- Many new definitions have been added e.g. consequence, impact, etc. and definitions of Risk Appetite, RPO, RTO, MAO, MTPD and MBCO *have been removed*. These changes will make BCMS universally applicable

  (**Important** Note - provided for the avoidance of doubt: The above comment is misleading. Whilst the above term and acronyms have indeed been [needlessly] removed from 'definitions' - they actually still exist, are fundamental [to business continuity] and should be used [just as before] in the theoretical and practical usage of all things 'business continuity')
- The addition to BIA is that the standard is now required to define impact categories and criteria which are relevant to the context - which in any case was being done
- *Deliberately Blank*
- Much of the detailing on how the context is to be set for BCMS has been removed giving more flexibility in implementation. Something similar is seen in section 7.4 on communication - the 2019 version being less prescriptive. Similar applies re the 'prescriptiveness' in Top Management commitment - where active participation of top management in an exercise program has been removed. Overall these changes make the standard more practical and pragmatic
- One of the ***very few*** new requirements is clause 6.3, which requires organisations to make changes to the BCMS "in a planned manner". Although technically this requirement is new, the content of the clause should not be a surprise to anyone
- Section 8.3 has been renamed from "Business Continuity Strategy" to "Business continuity strategies and solutions". This reflects the increased pragmatism of the standard: the focus is not so much on developing a grand strategy to ensure business continuity, but rather on finding solutions for specific risks and impacts

And another:

Below is from 22 May 2019 i.e. some 5 months before ISO 22301:2019 went live

The first edition of ISO 22301 was launched in May 2012. It was the first truly internationally accepted standard on business continuity, and it consists of requirements to implement a Business Continuity Management System according to ISO Annex SL. As such, it stood in line with prominent predecessors such as ISO 9001 and ISO/IEC 27001

When ISO/TC 292 (ISO Technical Committee 292 on Security and Resilience - responsible for the above standard) first asked within the community about the need to update it, there was astonishingly little response. We, as members, could not believe that no one had the intention or desire to update this international standard. However, the interest suddenly exploded and the respective ISO Project Team was challenged within an unprecedented volume of change requests concerning ISO 22301:2012

As of now, several modifications were integrated into the current DIS (Draft International Standard), and the process is not yet finished. During the revision process, a number of developments had to be observed

As ISO 22301:2012 was the first in a series of standards on business continuity developed by this TC, care had to be taken to synchronise modifications with the central glossary of this TC (ISO 22300) and auxiliary standards (technical specifications [TR]) developed ***after*** 2012 (e.g. standards on organisational resilience, business impact analysis, business continuity strategy etc.)

Here is a summary of current modifications and similarities ***as compared to the original*** *(2012)* ***version***:

- The PDCA model *diagram* was deleted, as diagrams are hard to standardise and typically lead to endless discussions and interpretations
- Clauses 4 to 10 still cover the components of PDCA, as before
- There are no normative references in this document
- The terms and definitions were updated to include the ISO Online Browsing Platform and the IEC Electropedia; both are web-based information platforms
- In clause 3 “Terms and Definitions” several terms were modified, redefined, removed and added. Major changes include: (see table *next* page)
- Clause 4 “Context of the organisation” received only minor modifications. The project team tried to create introductory sub-clauses at the beginning of each clause. As such, for example, sub-clause 4.1 is an introduction to clause 4 and sub-clause 4.2.1 (general) is an introduction to sub-clause 4.2.
- Clause 5 on leadership was streamlined.
- Clause 6 on planning was enhanced, focusing on business continuity objectives and planning to achieve them (6.2). A new sub-clause on planning changes to the BCMS (6.3) was introduced
- Clause 7 on support was streamlined

- Clause 8 (operation) took a lot of time to modify, as expected, addressing the core of the matter of business continuity. While the structure of the sub-clauses was ***not modified a lot***, new additions to the content were heavily discussed and, hopefully, improved to better suit the requirements of the practitioners who use this international standard e.g. sub-clause 8.2.2 "Business impact analysis" was enhanced and a reference to ISO 22318 (supply-chain continuity) was added. Notes referring to the terms MTPD and RTO (both removed from the clause on terms and definitions) were added

  Sub-clause 8.3, formerly called "Business continuity strategy" was renamed "Business continuity strategies and solutions", highlighting (in 8.3.2) the need for identification and selection of strategies and solutions. Clause 8.4 (formerly called "Establish and implement business continuity procedures") has been renamed to "Business continuity plans and procedures", focusing on "Response structure" (8.4.2), "Warning and communication" (8.4.3), "Business continuity plans" (8.4.4) and "Recovery" (8.4.5). A sub-clause on "Exercise program" (8.5) replaces the sub-clause formerly called "Exercising and testing"

- Clause 9 on "Performance evaluation" and clause 10 "Improvement" were streamlined, also taking into account the new requirements by ISO on how these clauses should look in order to be aligned with all ISO system management standards

Terms	Status	Terms	Status
consequence	introduced	supply chain	introduced
disruption	introduced	training	introduced
emergency	introduced	BCM	removed
impact	introduced	BCP	removed
information	introduced	document	removed
likelihood	introduced	infrastructure	removed
management	introduced	invocation	removed
measurement	introduced	MAO, MTPD, MBCO	removed
planning	introduced	risk appetite	removed
protection	introduced	BCMS	redefined
recovery	introduced instead of "RPO, RTO"	prioritized activities	changed to "prioritized activity"
resilience	introduced	product or service	slightly modified
review	introduced	testing	replaced by the term "test"

Ref table above - see also the associated '**important** note' page 126 - as it also applies here

And one more:

ISO 22301 Standard: new version 2019 for Business Continuity

Published on 30 June 2019

The initial version of ISO 22301 (2012) will be replaced in 2019 with a new version. The update ***does not include dramatic changes***, but it is an improvement that will produce greater value

Less definitions, more flexibility, more pragmatism, redundant sections reduced, definitions have become more consistent and the text is more logical

Among the changes to **DEFINITIONS** we have:

In clause 3 "Terms and Definitions", several terms were modified, redefined, deleted and added. The main changes include:

- ***INTRODUCTION*** of consequence, interruption, emergency, impact, information, probability, management, measure, planning, protection, resistance, review (update), supply chain, training, recovery instead of "RPO, RTO"
- ***ELIMINATION*** of the terms BCM, BCP, document, infrastructure, invocation, MAO, MTPD, MBCO, risk appetite

Ref the 2 bullet point entries (just above) - see also the associated '**important** note' page 126 - as it also applies here

- ***REDEFINITION*** of the term BCMS
- Prioritized activities ***CHANGED*** to "prioritized activity"
- The concept of product or service slightly ***MODIFIED***
- Testing ***REPLACED*** by the term "test"
- Notes were added with reference to the terms ***MTPD*** and ***RTO*** (*both deleted*)

In the 2012 version, "risk appetite" was defined as the "amount and type of risk that an organisation is willing to pursue or retain." The 2019 version removes all of the latter

The "appetite for risk" is not only a subjective issue, but, ultimately, also irrelevant. What matters is not the risk that an organisation is willing to take, but the level at which the impact of Resuming activities would be unacceptable for an organisation

The terms and definitions were updated to include the ISO Online Navigation Platform and IEC Electropedia; web based information platforms

Regarding changes in ***CONTEXT OF THE ORGANISATION***:

Requirements are reduced to the essentials for BCM. In Section 4.1 of the 2012 version, what the company must do and document to understand the organisation and its entire context is prescribed. In contrast, the 2019 version establishes the need to simply define and determine external and internal problems of the company and its context, but without specifying what this entails. It does not say what elements to consider, nor does it include requirements to document for this process

Similarly occurs in Section 7.4 on communication - the 2019 version is markedly less prescriptive

Regarding changes in ***LEADERSHIP***:

Clause 5 on Leadership was cut - participation of senior management (5.2). Senior management focused on what is necessary. Although in the previous version an active participation in the exercise and the test and all the stages was required, the new version is more pragmatic and focuses on what is really necessary to maintain the management system.

Regarding changes in ***PLANNING AND SUPPORT***

Clause 6 on Planning was improved, focusing on business continuity objectives and planning to achieve them (6.2)

A new sub-clause on change planning was introduced to the BCMS (6.3). It requires the company to make changes to the BCMS "in a planned way"

Clause 7 in Support was simplified

Regarding changes in ***OPERATION***

Clause 8 (Operation) addresses the core of business continuity. ***The structure of the sub-clauses was not significantly modified***. New additions to the content were improved e.g. sub-clause 8.2.2 "Analysis of business impact" was improved and a reference to ISO 22318 (continuity of the supply chain) was added

Section 8.2.2 on Business Impact Analysis (BIA) now stipulates that the ***BIA must take impact categories as a starting point***. Although many organisations already define impact categories in their BIA, the ***2019 version makes it mandatory***

In Section 8.3 the name "Business Continuity Strategy" has been changed to "Business Continuity Strategies and Solutions". This demonstrates pragmatism with an interest in finding strategies and solutions for possible impacts or specific risks (in 8.3.2), instead of concentrating on developing a great strategy to ensure continuity: ……"***The organisation must identify and select business continuity strategies based on the results of the business impact analysis and risk assessment. Business continuity strategies will consist of one or more solution***s…… "

Re 'Impact level versus ***not*** resuming an activity' - in the 2012 version, the amount and types of risks that a company is able to manage were defined. ***In the new version, the important thing is not the risk that it is willing to assume, but the level of impact that this risk may cause in the activities, and the impact that is generated to resume or not the activity***

Clause 8.4 (previously called "***Establish and implement business continuity procedures***") has been renamed to "***Business continuity plans and procedures***", focusing on "Response structure" (8.4.2), "Warning and communication" (8.4.3), "Business continuity plans" (8.4.4) and "Recovery" (8.4.5)

A sub-clause on "Exercise program" (8.5) replaces the sub-clause previously called "Exercise and test"

As for changes in ***IMPROVEMENT***

Clauses 9 on "Performance evaluation" and 10 "Improvement" were simplified, considering the new requirements to align with all ISO management system standards

TIMELINE and TRANSTION

More than 4000 companies have an ISO 22301 certificate (as at 2018)

The 2019 version of ISO 22301 was published on 31 October as 'ISO 22301: 2019'. There will be a transition period of three years. ***All certificates based on the 2012 version would lose their validity in the fall / autumn of 2022***

There are no major structural changes, which facilitates the transition for companies that already have certification

The PDCA model diagram was removed, since the diagrams are difficult to standardize and generally lead to endless discussions and interpretations

Appendix E

An Alternative to Using ISO (& Derivations) Published Standards & Supporting Documents

Firstly, take a look at the table below - and then continue reading on the next page:

Standard / Document	* **ISO Price** early **2020**	** **BSI Price** early **2020**
Business Continuity Related Standards etc.		
ISO 22300:2018	GBP 29	GBP 206
ISO 22301:2019	GBP 91	GBP 178
ISO 22313:2020	TBA	TBA
ISO 22317:2015	GBP 106	GBP 206
ISO 22318:2015	GBP 91	GBP 206
ISO 22330:2018	GBP 122	GBP 232
ISO 22331:2018	GBP 91	GBP 206
ISO 22332:2020	TBA	TBA
Totals	GBP 530	GBP 1234
Risk Management Standards etc.		
ISO 31000:2018	GBP 68	GBP 132
ISO 31010:2019	GBP 152	GBP 304
ISO Guide 73:2009	GBP 68	GBP 176
ISO 31703	TBA	TBA
Totals	GBP 288	GBP 612
Grand Totals	GBP **818**	GBP **1846**

Diff = GBP 1028 (1846 minus 818) i.e. BSI bought standards (as listed above) cost about ***226% more*** (in total) than the equivalent ISO bought standards indicated above

* Converted from CHF to GBP. Exchange rate 1GBP = 1.3 CHF (Latter is approximate [average] exchange rate for year 2019)

** Prices are for ***non***-BSI members

Note: BSI (British Standards Institution) is the national standards body of the United Kingdom. It sells ISO standards under its own name and at its own prices - as can be seen from the table above. A number of other countries around the world do likewise e.g. ANSI in the USA; EVS in Estonia etc. BSI prices (for selling exactly the same standards as can be purchased from ISO) are significantly more expensive for non-BSI member purchasers

Part 1 - Background

ISO must have had a basic logic and thinking problem (or worse) when it produced (in 2012) its first business continuity standards in the series starting with the first two numerals '22' (as in ISO ***22***301 and ISO ***22***313 - both relating to 'Business Continuity')

The problem was not with ISO 22301:2012 itself as it (itself) was the associated ***requirements*** standard i.e. it contained only the requirements (nothing more) which an organisation needed to meet in order to become ISO certificated (to that standard) or to make a self-declaration of alignment with same

There was, however, a **BIG** problem with ISO 22313:2012 - which was supposed to have been the ***guidance*** document on ***how to implement*** ISO 22301 - the problem being that ISO 22313 was ***not fit for this purpose***

Accordingly, anyone wanting to certificate an organisation to ISO 22301 would have needed to obtain the required guidance from other sources - particularly (non-ISO produced) subject matter commercial publications available at the time (there weren't many of them about) - and also from subject matter experts (already having a background of business continuity expertise - built up prior to the 2012 publication of ISO 22301 e.g. by working with one of the latter's main predecessor standards e.g. BS 25999)

The latter publications and expertise needed to be paid for of course (i.e. over and above the not insubstantial costs of purchasing ISOs 22301 and 22313 in the first place)

Furthermore, as ISO did not have the good grace to include an associated vocabulary in either of the latter two documents - this (vocabulary) also required purchase (ISO 23000 - first published in 2012 / latest version 2018)

Note: The reader might wonder how the author of this CRPM Part 3 / Volume 1 (you are reading it now) knows all of the above. The answer is that he experienced exactly the problems (as have just been described just above) when trying to put his own (first edition) 'guideline / guidance' Business Continuity Plan together - in October 2012 (see 'revision history' page 3)

It took ISO 3 years to *indirectly* acknowledge the inadequacy of its ISO 22313 guidance standard - evidenced in 2015, when it published supplementary (additional) guidance standards:

- 'Business Impact Analysis (BIA) - ISO 22317' and
- 'Supply Chain Continuity' - ISO 22318'

Both required ***additional*** purchase (from ISO or its agents) of course. Take a look at the table on the previous page to see where they 'fitted-in' - together with their late 2019 prices

Fast-forwarding to 2018, ISO filled in more of the ISO 22313 cracks by kindly offering customers the opportunity to buy ***additional*** (newly written) supplementary guidance standards:

- 'People Aspects of Continuity - ISO 22330' and
- 'Business Continuity Strategy - ISO 22331'

It also took the opportunity to update ISO 23000 ***and sell it all over again*** (as a matter of interest note [from table on page 132 and as one example only], the huge difference in ISO and BSI prices for this document!)

In late 2019 / early 2020, the ISO 'money / gravy-train' rolled on - as ISOs 22301 and 22313 were updated and re-issued (i.e. '***sold***' [Yes! they had to be purchased all over again - despite the subsequent and well published information provided by several subject matter experts ***at the time*** {see Appendix D of this document - page 125 for a reminder of the latter - if required} - that '***there had been no really significant changes***' in these updated versions - compared to their predecessor versions of 2012])

More particularly, the opportunity at that time to reposition / include / incorporate the five supplementary documents (ISOs 223000, 22317, 22318, 22330 and 22331) (+ ISO 22332 [Business Continuity Plans / Procedures] due for issue sometime in 2020) into / in the updated ISO 22313:2020 (where they really belonged of course because it [ISO 22313] was supposed to provide guidance to meeting the requirements of ISO 22301) was missed (the more cynical reader might think that this was deliberate!)

And - you might have guessed it! - ISO then used the above as an opportunity for all organisations ***already having*** ISO 22301 certification (believed to be around 4,000 around the world in late 2019) to have to ***re-certificate*** to the 2019 version within 3 years i.e. by about November of 2022

*Note: Costs associated with obtaining ISO certification (to a specific standard such as ISO 22301) are significant, particularly for larger organisations (where they can be **very** significant)*

*Whilst **re**-certification should obviously be cheaper (compared to the initial certification process) - it might still be considered a 'waste of time, effort and money' so to do - due to the lack of significant change (as already mentioned above) from the previous versions of ISOs 22301 & 22313 (**+** the fact that - at the end of 2019 - ISOs 223000, 22317, 22318, 22330 and 22331 were still extant, as per the versions shown in the table on page 132)*

The reader should also note that, in the meantime, a significant, 'commercial' (for profit) business / trade (with many different providers [some good and some not so good] worldwide) had gradually built up (not including ISO itself - which only produces and sells its own standards [e.g. it does not conduct associated training, certification etc]) to sell anything (e.g. text books, software; certification, training etc.) to do with Business Continuity

The latter was initially needed because (as we have seen) ISO 22313:20***12*** did not deliver what was required of it. By 2020 such business / trade had become (and still is) a self-sustaining reality - which is good of course as the ISO 22313:2020 version similarly failed to 'deliver'

However, the most significant reason for such commercial businesses / trade thriving (even with ISOs 223000, 22317, 22318, 22330, 22331 & 22332 being available [which, the reader will recall - did not start happening until 2015]) is because one can only get so much from a book[s] / documentation etc. - including the document you are reading right now e.g. would you really be able to fly an aeroplane safely just by reading the associated flying manuals only!!!

It might now be worth taking another look at the note found on the bottom of page 2 of this guideline (you are reading the latter now) + the associated 'purpose & scope' starting page 50

Last point here is that ***Business Continuity*** (BC) is (without argument - no matter what BC professionals / practitioners might say) simply a **sub-component** of ***Risk Management*** (RM). Anyone serious about BC should thus clearly understand that he / she / they also need to have an appropriate level of knowledge and experience of the associated aspects of RM - in order to successfully and efficiently conduct (other than relatively simple) BC activities

One building block (of several) related to what is written in the last para above is to acquire and retain the theoretical knowledge required - and, of course, this then translates as another 'money-maker' for ISO in that the associated requirement standard (ISO 31000) + its guidance standard (ISO 31010) + the associated vocabulary (ISO Guide 73 / ISO 31703 from 2020) will all need to be purchased or otherwise made available. See table on page 132 for late 2019 prices

Part 2 - There is an Alternative

There can be no doubt whatsoever that ***adopting*** business continuity (BC) related measures into the vast majority of activities (whatever they might be) conducted by organisations (whoever and whatever type they might be [including 'simple, single person' organisations as appropriate]) will be beneficial to said organisations

The same cannot be said (with a relatively small number of notable * exceptions) for the need to ***certify*** any organisation's activities to the ISO 22301 BC requirements standard

* For example, ISO 22301 certification by 'supply-chain' type organisations would almost certainly lead to more 'quality and quantity' business (all other matters being equal), thus probably more profit etc.

Instead, it is proposed herein that most organisations could achieve the same result (but without all of the ISO related expenses and 'hassle') by ***aligning*** (instead of ***certifying***) their concerned activity / activities - with ISO 22301. This is probably best achieved by a formal 'self-declaration' (by said organisations) of such alignment

Of course, much of the same work (as per the 'formal' ISO route) ***would still need to be accomplished***, but now without the rigidity (and possibly the slight intimidation?) of the ISO certification process overshadowing the project - and most definitely at a ***significantly lower*** financial commitment by the organisation, for the same result

As to a documented guide (text book) to achieving the above, the below boxed note is repeated from page 35:

> Of course, there ***is*** also a **FREE** resource available which provides what is needed. **You are reading** (Volume 1 of) **it right now**! (It is about 80% generic and 20% aviation related - so should still be very useful to most organisations - even if they lie outside of the aviation industry)

Taken together, both volumes (again - you are reading Vol 1 right now [Volume 2 being a ***separate*** and ***much more detailed*** guideline document]) of this CRPM Part 3 guideline document should provide you with much of the guidance you need. If your interest is not aviation related, it is suggested that you take action to make the appropriate adjustments accordingly

You might occasionally need to consult one or other of the documents shown in the table on page 132. If you search hard and long enough you will probably be able to come up with something useable from the internet. For example, the full ISO 223000:2018 (BC Vocabulary) was available (on the internet [read only]) at time of writing at:

https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en

If you purchase the latter from ISO it would cost (as at late 2019) GBP 29. The UK's British Standards Institute (BSI) would have charged you GBP 206!!! ***This document comprises just 35 pages!!!!!!***

Note: With the passing of time you will find that internet links (such as the one given just above) will cease working. As mentioned, a conscientious internet search (using appropriate keywords) should generally (but not always) lead you to what you are looking for

However, and as an example of how useful this CRPM guideline (reminder - you are reading Vol 1 of it right now) might be to you, all of the appropriate vocabulary from ISO 23000 is already included herein - with much of it providing ***additional*** and ***valuable*** meaning / common sense interpretation / expansion (over and above what ISO 23000 provides)

Deliberately Blank

Conclusion

That's it for CRPM Part 3 / Volume 1

If you now wish to commence the real task of preparing, implementing etc. a BCMS for your organisation (particularly if your organisation is an airline, airport, ground handler etc.) see (separate but related document):

CRPM PART 3 / ***VOLUME 2***

You can find the latter via:

https://aviationemergencyresponseplan.com/aviation-business-continuity/

Note:

Concerning BC planning for ***airports in the USA***, a useful (if slightly dated) reference document was published in late 2013. Much of its content will no doubt still be relevant today - not just in the USA but often worldwide. It can be downloaded at:

http://www.trb.org/Publications/Blurbs/169246.aspx

If the above link does not work, conduct an internet search for:

'……. ACRP Report 93: Operational and Business Continuity Planning for Prolonged Airport Disruption - 11/7/2013 (7 Nov 2013) …….'